ERROR CORRECTING CODES ON ALGEBRAIC SURFACES

A Thesis

Submitted to the Faculty

of

Purdue University

by

Chris C. Lomont

In Partial Fulfillment of the

Requirements for the Degree

of

Doctor of Philosophy

May 2003

To dad, whose interest in science inspired mine,

and mom, whose support and encouragement made this possible

ACKNOWLEDGMENTS

I would like to express my sincere thanks to my advisor, Professor T.T. Moh, for the guidance, encouragement, and support during my coursework and research. I also wish to thank Professors William Heinzer, Brad Lucier, and Kenji Matsuki, for serving on my committee and for discussing all the countless questions and topics I brought to them. I especially thank Kenji Matsuki for helping me to learn Algebraic Geometry from Hartshorne's book, which made this thesis possible.

I thank my parents, Mary Lou and Kent, for encouraging me into science, and for all the creative things they stimulated me with growing up. I also thank them for allowing all the crazy ideas I pursued, all the experiments I performed on household items, and all the fun things my siblings and I got to do as children.

I thank my many friends and peers at Purdue. Among them I thank Roy Osawa for early guidance, Mark Rogers for rooming with me 4 years and all the work we put in learning aspects of ring theory, Chris Mitchell for many topics of discussion, and Charles Crosby for watching countless movies with me. I thank Jimmy Chen, who has been a student of Professor Moh along with me, and who has attended and talked at our many seminars on aspects of coding theory, cryptography, and other areas of math.

I thank my officemate and friend of 7 years, Majid Hosseini, who went through the entire process with me, inspired me, listened to me, pushed me, and spent many hours talking math, hiking, and enjoying life with me.

These last few years I especially thank Melissa Wilson, wonderful girlfriend, fiancee, and soon to be wife, who has given me reason to work harder, try to achieve more, and who causes my life to be immensely richer.

Finally, I would like to thank all the video game developers worldwide, who have given me plenty of distraction my many years at Purdue. In particular, the makers

of Heroes of Might and Magic I, II, and III, the makers of Doom and Quake, and the makers of various online chess games. Without them I would have graduated much sooner and missed meeting some people important to me.

TABLE OF CONTENTS

Page

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Lomont, Chris C.. Ph.D., Purdue University, May, 2003. Error Correcting Codes on Algebraic Surfaces. Major Professor: Tzuong-Tsieng Moh.

Error correcting codes are defined and important parameters for a code are explained. Parameters of new codes constructed on algebraic surfaces are studied. In particular, codes resulting from blowing up points in $\mathbb{P}^2$ are briefly studied, then codes resulting from ruled surfaces are covered. Codes resulting from ruled surfaces over curves of genus 0 are completely analyzed, and some codes are discovered that are better than direct product Reed Solomon codes of similar length. Ruled surfaces over genus 1 curves are also studied, but not all classes are completely analyzed. However, in this case a family of codes are found that are comparable in performance to the direct product code of a Reed Solomon code and a Goppa code. Some further work is done on surfaces from higher genus curves, but there remains much work to be done in this direction to understand fully the resulting codes. Codes resulting from blowing points on surfaces are also studied, obtaining necessary parameters for constructing infinite families of such codes.

Also included is a paper giving explicit formulas for curves with more $\mathbb{F}_q$-rational points than were previously known for certain combinations of field size and genus. Some upper bounds are now known to be optimal from these examples.

(This page deliberately left blank.)

1. INTRODUCTION

"Mathematics is an interesting intellectual sport but it should not be allowed to stand in the way of obtaining sensible information about physical processes." Richard W. Hamming

Redundant information is almost a necessity in any area of communication. For example, the text "CN U RD THS? THN U R ERRR CRRCTNG" is still readable to most people, who process these words, mentally adding missing letters as necessary. ISBN numbers on books are engineered to detect if any digit is incorrect, and to detect any transposition of digits. UPC codes are designed to detect errors. Many areas of natural communication use error correction, and certainly technological communication would be impossible without it.

Transmitting information is one of the cornerstones of modern technology. Due to inherent noise, this information must be protected against corruption, and the most obvious way is to send multiple copies of the data, then choosing the most common outcome, a method called the "repetition code".

The disadvantage of repetition codes is that the overhead of sending multiple copies of the information becomes unacceptably high. While working at Bell Labs in the USA in 1948, Dr. Claude Shannon published "A Mathematical Theory of Communication," starting information theory by showing that it was possible to encode information such that the overhead was minimal [47]. Unfortunately his proof was not constructive, leaving room for later researchers to seek these promised codes.

Two years later, Richard Hamming, also at Bell Labs, constructed the simple codes bearing his name [20] that take four data bits, add three check bits, and allow the correction of any single bit error. The repetition code above would require twelve bits to do this, so Hamming codes began the realization of more efficient coding methods.

Besides Shannon and Hamming, many of the pioneers in information theory worked at Bell Labs too: Berlekamp, Gilbert, Lloyd, MacWilliams, and Sloane.

As these events unfolded, John Leech at Cambridge created similar codes while working on group theory. His codes were based on the remarkable 24-dimensional Leech Lattice, and were related to sphere packings (which have become essential to coding theory). This lattice was also important to the classification of finite simple groups.

The most widely used class of error correcting codes, Reed-Solomon codes, were introduced by Irving S. Reed and Gus Solomon in a 1960 paper entitled, "Polynomial Codes Over Certain Finite Fields," while they were on staff at the Massachusetts Institute of Technology's Lincoln Laboratory [42]. These codes have good properties for many small fields used in practice, and have efficient decoding algorithms, making them indispensable to engineers for the past several decades.

The utility of error correcting codes for information transmission was immediately apparent, and was used by NASA in all space programs. For example:

In 1965 the NASA Mariner probe took photos of Mars at 200x200 resolution in 64 grey levels (6 bits), transmitted 8 bits per second, and required 8 hours to transmit a picture [39]. The Mariner probe in 1969 used a Hadamard code with a rate of 6/32, and was able to correct up to 7 errors in a received word of 32 symbols [30, 2.1, 4.1]. From 1969 to 1973 NASA used a binary (32,64,16) Reed-Muller code which could correct 7 out of 32 bits, detect 8 errors, using 6 data bits and 26 check bits. Transmission was increased to 16000 bits per second. In January 1972 Mariner 9, the first spacecraft to orbit another planet, used this code on 600x600 pixel pictures, taking in 100,000 bits per second at the camera, so had to store pictures for later transmission [43, Ex 4.2.2] [39]. In 1976, Viking landed on Mars, and took color pictures [43]. From 1979-1981, Voyager spacecrafts took color Jupiter and Saturn pictures, using a 4096 symbol alphabet (4 bits each of red, green, and blue: $2^{12} = 4096$) to send color, using a binary (24,4096,8) Golay [15] code, which is 3 error correcting and 4 error detecting, with rate R=12/24 [43, Ex 4.2.3]

Modern consumer devices are riddled with error correcting schemes. Modems on computers use codes to fight phone line noise. Compact Discs (CDs) use a Cross Interleaved Reed Solomon Code (CIRC) to protect against scratches, dirt, and cracks, and will correct up to about 4000 consecutive errors (about 2.5 mm of track). Audio systems can overcome even more damage by interpolating the signal [37]. Computer hard drives use a Reed Solomon code to fix errors on platters. DVDs, satellites, fax machines, and telecommunications equipment all use error correcting codes. DARS (digital audio radio services) and SDARS (satellite digital audio radio services) rely on error correction to create CD quality radio. For example, the new subscription digital radio band, XM, at 2332.5 to 2345 MHZ, has 50 CD quality (64kb/s) channels and many lower quality channels, and uses a Reed Solomon outer code with a 1/2 convolutional inner code [53]. HDTV (High Definition Television) has error correcting codes built into the specifications. A Yahoo search on "error correcting code" yielded 14900 hits; searching for "coding theory" yielded 33,200 hits (Mar 2003). Researchers think perhaps DNA uses error correction to avoid fatal defects [33]. Internet transmission uses error correction at many levels.

Perhaps the most interesting area where error codes are being applied is in quantum computing. Due to the very sensitive nature of quantum states, quantum computers have very special requirements to maintain data integrity. Numerous researchers have worked on error correcting codes to make quantum computation feasible, [48, 6, 5], and it was while studying quantum computing that I became interested in error correcting codes.

This thesis is concerned with constructing new classes of error correcting codes, deducing their parameters, and finding better codes usable in the future, since current codes are losing some of their usefulness as data rates increase and demands become more stringent. Theoretically, the best class of codes currently are the Goppa codes, which are codes from linear systems on algebraic curves. Their usefulness comes from the many $\mathbb{F}_q$ rational points on curves of large genus and some deep properties about modular curves. Since higher dimensional varieties would have even more $\mathbb{F}_q$ points, I

wanted to mimic for surfaces some of the constructions on linear systems from curves, to see if I could obtain better codes.

In particular, by examining codes coming from ruled surfaces I was able to construct some codes that are better than the direct product of Reed Solomon codes over a fixed field. This was done by classifying all such codes from surfaces ruled over $\mathbb{P}^1$. Also codes on surfaces ruled over an elliptic curve are studied, and partial results are obtained, giving another class of codes that have good parameters.

Blowing up points on surfaces to obtain long families of codes is briefly studied, but turned out to be a difficult path to analyze. Necessary conditions are found to construct such families of codes.

Finally, new curves are explicitly given that have more $\mathbb{F}_q$ rational points on them than were previously known for certain genus and q combinations. In some cases this increases the number of points to match known bounds, showing that the bounds cannot be improved for those combinations.

The layout of this thesis is as follows. Chapter 2 contains basic error correcting coding background. Chapter 3 covers some theorems giving sufficient conditions to construct codes on higher dimensional varieties. Chapter 4 is an initial attempt to construct codes on families of surfaces by blowing up points. Chapter 5 covers constructions on ruled surfaces, and in particular, constructs 2 families of codes with explicit parameters. This is done by classifying all codes on surfaces ruled over $\mathbb{P}^1$, which gives codes slightly better than the product code of two Reed Solomon codes. The other family is over certain surfaces ruled over an elliptic curve, and these codes are also comparable to the corresponding product code. Chapter 6 contains new curves with many rational points, and compares them to bounds on the number of rational points. Chapter 7 is the conclusion and lists some open problems.

2. CODING THEORY BACKGROUND

2.1 Error Correcting Codes

An error correcting code is a method of adding redundancy to data, so that if the resulting redundant data gets corrupted, the original data can be reconstructed from the corrupted data. A linear error correcting code (LECC) is a subspace C (the *codewords*) of a vector space V over some finite field $\mathbb{F}_q$. Let $n = \dim V$ (the *length* of the code), $k = \dim C$ (the *dimension* of the code), and then denoting $c = (c_1, c_2, \ldots, c_n) \in C$, let $d = \min\{\#c_i \neq 0 \mid c \neq 0 \in C\}$ (the *distance* of the code). C is called an $[n, k, d]$ code. The vector space $\mathbb{F}_q^k$ (elements are called *messages*) can be embedded in V with image C. This embedding adds the redundancy needed to correct errors. Given a vector $m \in C$ (a codeword), and arbitrarily changing at most $t = \lfloor \frac{d-1}{2} \rfloor$ entries in m to get an element $r \in V$ (the received word), then m is the unique codeword in C that differs from r in at most t places. Given $r \in V$, finding such $m \in C$ is called decoding. Creating efficient decoding algorithms is usually separate from constructing good codes.

Note 2.1.1 For this thesis, the word "code" will denote a linear error correcting code, unless otherwise stated.

2.2 Parameters of a Code

Important parameters of an error correcting code are the rate $R = \frac{k}{n}$ and the relative error correcting capability $\delta = \frac{d}{n}$. Both values are in $[0, 1]$, and both are desired to be as large as possible. Of course as one value increases, there are bounds forcing the other value to decrease. It is a hard open problem to understand completely this relationship for general codes.

2.2.1 Shannon's Noisy Coding Theorem

Shannon's Noisy Coding Theorem [47] says (roughly) that given any rate R less than the maximal rate a channel can support (which we leave undefined for this thesis, however see [43]), and any decoding failure probability $p > 0$ desired, there exists a code with rate R and probability of failure $< p$ (which depends on δ and the channel noise), if *the length of the code is allowed to grow arbitrarily.* Explicit construction of such codes is unknown; since such codes must be very long, long families of codes are often studied. Finding codes promised by Shannon's Theorem is a central problem in coding theory. As a result of this theorem, people are led to look at families of codes, whose lengths tend to infinity.

Thus the definition:

Definition 2.2.1 *A* **good family** *of codes is a sequence* $C_1, C_2, \ldots, C_n, \ldots$ *of codes over a fixed* $\mathbb{F}_q$ *such that both* $\limsup \delta(C_n)$ *and* $\limsup rate(C_n)$ *are bounded away from 0, and* $\lim_{n\to\infty} length(C_n) = \infty$.

For a fixed $\delta \in [0, 1]$, finding a good family of codes with the highest asymptotic rate R is an important theoretical question, but is in general unsolved. This highest value is often denoted $\alpha(\delta)$ or $\alpha_q(\delta)$ (over an alphabet with q elements) (see [30, Ch. 5]).

2.2.2 Upper Bounds

There are relations for possible values of n, k, and d. For example, for an $[n, k, d]$ code, the Singleton Bound is [30, Cor 5.2.2])

$$n + 1 \geq k + d \tag{2.1}$$

The singleton bound leads to an upper bound of $\alpha(\delta) \leq 1 - \delta$. There are many bounds improving on this, see for example [43] and [30].

2.2.3 Lower Bounds

Lower bounds are important since they guarantee existence of a family of codes. One of the best bounds is the Gilbert-Varshamov (GV) bound [43, Theorem 4.5.26]:

Theorem 2.2.1 (Gilbert-Varshamov Bound) *For an alphabet of q symbols (e.g., a finite field $\mathbb{F}_q$), let $\theta = \frac{q-1}{q}$. **If** $0 \leq \delta \leq \theta$ **then***

$$\alpha_q(\delta) \geq 1 + \delta \log_q \delta + (1-\delta) \log_q (1-\delta) - \delta \log_q (q-1)$$

Their method is constructive, yet not efficient for implementation, thus leaving room to find efficient codes. However for about 30 years, researchers doubted this bound could be improved, and were surprised when it was surpassed by Goppa codes (see section 2.4 below).

2.3 Direct Product Codes

Let C_i be an $[n_i, k_i, d_i]$ code with rate R_i and relative distance δ_i, for $i = 1, 2$, over the same field $\mathbb{F}_q$. Since the code C_i takes a vector of length k_i and encodes it into a vector of length n_i, it is natural to define a product code $C = C_1 \times C_2$ as follows: take as a message a $k_1 \times k_2$ matrix over $\mathbb{F}_q$. Encode each row using the code C_1 to get a $n_1 \times k_2$ matrix, then apply C_2 to encode each row, resulting in a codeword in C, which is viewed as a $n_1 \times n_2$ matrix. With setup we have

Theorem 2.3.1 *Given $[n_i, k_i, d_i]$ codes C_i with rates R_i and relative distances δ_i, $i = 1, 2$, the **direct product code** $C = C_1 \times C_2$ is an $[n_1 n_2, k_1 k_2, d_1 d_2]$ code. In particular it has rate $R_1 R_2$ and relative distance $\delta_1 \delta_2$.*

Proof See [30, ex 3.8.12]. The proof is an exercise, with a solution in the back of the book which would take us too far afield. ■

Definition 2.3.2 *For the rest of this paper direct product codes will be called merely "**product codes**".*

Since rates and relative distances are in $[0,1]$, product codes never increase the rates or error capabilities. However, there are often other reasons to mix codes: for example, to fight long burst errors in CD players and space satellites, or to combat other types of errors due to engineering constraints. For methods of combining codes to obtain new codes see [43, Ch 4.3].

2.4 Codes from Curves

Probably the most commonly used codes are the Reed Solomon (RS) codes, which, over a finite field $\mathbb{F}_q$ of q elements, give codes with parameters $[q-1,k,q-k]$, $0 \leq k \leq q-1$. Note these meet the Singleton Bound (equation 2.1), but suffer from being a fixed length for a given field. In 1981 Goppa [16] generalized RS codes to codes on algebraic curves, with the RS codes being the Goppa code over the curve $\mathbb{P}^1$. Using the Riemann-Roch theorem [30, 10.5.1] to deduce the parameters, a curve of genus g with n distinct $\mathbb{F}_q$-rational points gives $[n-1, m-g+1, n-m]$ codes, for $2g-2 < m < n$.

Briefly, let X be a nonsingular curve of genus g over $\mathbb{F}_q$, with distinct $\mathbb{F}_q$-rational points $P_0, P_1, \ldots, P_n$. Let divisors $D = P_1 + P_2 + \cdots + P_n$ and $G = mP_0$, with $2g-2 < m < n$, and let K be the canonical divisor. Let the code C be the image of $\alpha : \mathcal{L}(G) \to \mathbb{F}_q^n$ given by $\alpha(f) = (f(P_1), f(P_2), \ldots, f(P_n))$. If $f \in \ker \alpha$ then f has $\geq n$ zeros, but the number of poles of f is $\leq m < n$ which implies $f = 0$. Thus $m < n \Rightarrow \alpha$ is injective. Riemann Roch gives $\dim(G) - \dim(K-G) = \deg(G) - g + 1 = m - g + 1$ so the dimension $k = \dim(G)$ of the code is at least $m - g + 1 + \dim(K-G)$. When $\dim(K) = 2g-2 < m = \deg(G)$, this reduces to $d \geq m - g + 1$.

Suppose $\alpha(f)$ is nonzero, with d nonzero entries. Then f has $n-d$ zeros among the P_i, so has a pole of order at least $n-d$ at P_0, forcing $\deg G \geq n-d$, so the bound on the distance is $d \geq n - \deg G = n - m$. This guarantees a $[n, m-g+1, n-m]$ code.

Bounds on the length of such codes are discussed in my paper [31], which is reproduced in chapter 6.

Note 2.4.1 The Riemann Roch theorem will be used throughout this paper, as stated in [22, IV, Theorem 1.3] or [30, 10.5.1]

Note 2.4.2 Unless otherwise stated, all varieties and bundles in this paper will be defined over a finite field $\mathbb{F}_q$. In particular every variety is assumed to have at least one $\mathbb{F}_q$ rational point.

Surpassing the GV bound was thought impossible for over 30 years, until 1982, when Tsfasman, Vlăduţ, and Zink [50] used modular curves [35] to construct Goppa codes surpassing the GV bound, giving the TVZ bound:

Theorem 2.4.3 (TVZ Bound) *Fix a finite field* $\mathbb{F}_q$*. Let* $\gamma = (\sqrt{q} - 1)^{-1}$*.* ***Then***

$$\delta + \alpha_q(\delta) \geq 1 - \gamma$$

Drinfeld and Vlăduţ [10] showed that the TVZ bound is the best possible using Goppa codes.

See Figure 2.1 for a graph showing the Singleton, Gilbert-Varshamov, and TGV bounds when $q = 121$. It shows a graph of the requested relative distance $d = \delta$ versus the asymptotic rate $a = \alpha(\delta)$ for an infinite family of codes. Note for some values of d that the TVZ bound exceeds the GV bound.

2.5 Codes from Higher Dimensional Varieties

Tsfasman [49] generalized the Goppa construction to arbitrary varieties as follows:

Definition 2.5.1 (Code definition) Let X be a normal projective variety over a finite field $\mathbb{F}_q$, and let L be a line bundle on X also defined over $\mathbb{F}_q$. Given $P_1, P_2, \ldots, P_n$

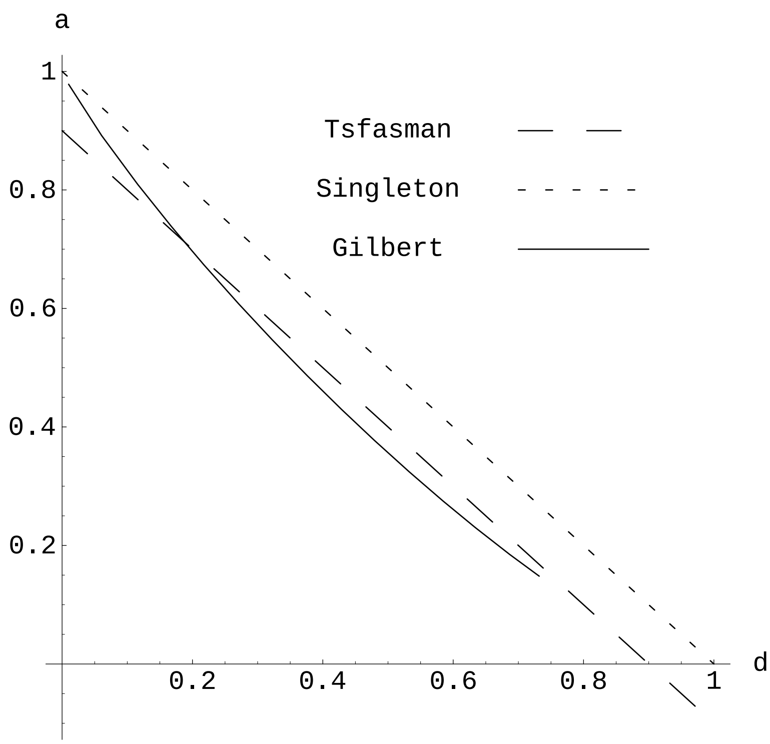

Figure 2.1. Bounds on Parameters of Codes

distinct $\mathbb{F}_q$-rational points on X, fix isomorphisms $L_{P_i} \cong \mathbb{F}_q$ at each stalk. Define the **code** $C(X, L)$ as the image of the germ map

$$\alpha : \Gamma(X, L) \to \bigoplus_{i=1}^{n} L_{P_i} \cong \mathbb{F}_q^n$$

This map is evaluation of a section at each P_i, and gives a vector space over $\mathbb{F}_q$.

The main problems are making sure α is injective and estimating the distance of the code. To compute the distance, we need to know: given $s \neq 0 \in \Gamma(X, L)$, how many zeros does s have among the P_i? One tool to approach this question is intersection theory, as in [12].

For curves, these bounds are straightforward to derive using Riemann-Roch as shown above, but this approach fails for higher dimensional varieties.

The only work I know of studying codes from higher dimensional varieties in some depth is the 1999 thesis of S. Hanson [21]. Using theorems from this I analyzed several classes of codes on surfaces, and classified some explicit cases. See the last few paragraphs of the introduction for a synopsis of what will follow.

Note 2.5.2 For the rest of this paper, α will be the germ map, NOT the function $\alpha(\delta)$ relating the relative rate R and relative distance δ for families of codes.

(This page deliberately left blank.)

3. THEORY ON VARIETIES

3.1 Introduction

Here are reproduced theorems that give the background for the work that follows. Codes will be constructed by the method in definition 2.5.1. In particular, sufficient conditions are found guaranteeing that the germ map is injective, and bounds are obtained on the distance of the resulting codes. Also, minor corrections and changes from [21] are stated.

3.2 Theorems

This first theorem gives a bound on the distance of codes on higher dimensional varieties.

Theorem 3.2.1 *[21, Theorem 5.9] Suppose X is a normal and projective variety over $\mathbb{F}_q$, $\dim X \geq 2$, and $C_1, C_2, \ldots, C_\gamma$ are irreducible curves on X with $\mathbb{F}_q$-rational points $P_1, P_2, \ldots, P_n$. Assume there are $\leq N$ points on each C_i. Let L be a line bundle such that $L.C_i \geq 0$ for all i. Let*

$$l = \sup_{s \in \Gamma(X,L)} \#\{i : C_i \subseteq Z(s)\}$$

where $Z(s)$ is the divisor of zeros of s.

***Then** the code $C(X, L)$ has length n and minimum distance*

$$d \geq n - lN - \sum_{i=1}^{\gamma} L.C_i$$

If** $L.C_i = \delta \leq N$ for all i **then

$$d \geq n - lN - (\gamma - l)\delta$$

Proof Let $s \in \Gamma(X, L)$. Let D be its divisor of zeros. $\alpha(s) \in \mathbb{F}_q^n$ has $\#(D \cap \cup_i C_i)$ $\mathbb{F}_q$-zero coordinates. $D \cap (\cup_i C_i) = (\cup_{C_i \subseteq D} C_i) \cup (D \cap \cup_{C_i \nsubseteq D} C_i)$, where the last intersection is proper. So $\alpha(s)$ has at most $lN + \sum_{C_i \nsubseteq D} L.C_i$ zeros. $L.C_i \geq 0$, so the last formula is bounded by $\sum_{i=1}^{\gamma} L.C_i$, implying

$$d \geq n - lN - \sum L.C_i$$

If each curve counts the same in the intersection product ($L.C_i = \delta$), then we can correct for double counted zeros by subtracting $l\delta$ from the possible number of zeros:

$$d \geq n - lN - (\gamma - l)\delta$$

■

Corollary 3.2.2 *[21, Cor 5.10]* ***If*** $n > lN + \sum_i L.C_i$ ***then*** *α is injective.*

Proof The distance $d > 0$ implies injectivity. ■

Corollary 3.2.3 *[21, Cor 5.11]* ***If*** *X is a nonsingular surface, H is a* nef *divisor on X with $H.C_i > 0$* ***then***

$$l \leq \frac{L.H}{\min_i\{C_i.H\}}$$

Thus ***if*** *$L.H < C_i.H$ for all i,* ***then*** *$l = 0$ and $d \geq n - \sum_{i=1}^{\gamma} L.C_i$*

Note 3.2.4 H nef (numerically effective) means $H.C \geq 0$ for all curves C on X.

Proof Let D be a member of the linear system L corresponding to covering l of the C_i. Then H nef $\Rightarrow L.H = D.H \geq \min\{C_i.H\}l \Rightarrow$

$$l \leq \frac{L.H}{\min\{C_i.H\}}$$

■

The above proves

Theorem 3.2.5 (Main Theorem) *[21, Theorem 5.1] Let X be a nonsingular projective surface over $\mathbb{F}_q$. Let $C_1, C_2, \ldots, C_\gamma$ be irreducible curves on X with $\mathbb{F}_q$ rational points $P_1, P_2, \ldots, P_n$. Let L be a divisor on X with $L.C_i \geq 0$ for each i. Let H be a divisor on X so that H is nef and $H.C_i > 0$. Assume $L.H < C_i.H$ for all i.*

***Then** the code $C(X, L)$ has length n, minimum distance $d \geq n - m$ where $m = \sum L.C_i = \sum \deg_L(C_i)$, and **if** $m < n$, **then** the dimension of C is $k = \dim_{\mathbb{F}_q} \Gamma(X, L)$.*

Note 3.2.6 Hanson [21] leaves out the word "irreducible" and requires H is ample and L is nef. However, the above conditions are strong enough to prove the theorem.

Note 3.2.7 Bjorn Poonen [38, Cor 3.5] has shown existence of *space filling curves* with the following:

***Corollary 3.2.8** Let X be a smooth, projective, geometrically integral variety of dimension $m \geq 1$ over $\mathbb{F}_q$, and let E be a finite extension of $\mathbb{F}_q$. Then there exists a smooth, projective, geometrically integral curve $Y \subseteq X$ such that $Y(E) = X(E)$.*

The methods in that paper [38] can perhaps be extended to find coverings of surfaces by curves each with an equal number of rational points, allowing the second bound on the distance from theorem 3.2.1 to be used.

(This page deliberately left blank.)

4. CODES FROM BLOWING UP POINTS ON SURFACES

4.1 Long Codes

In order to obtain good families of codes (definition 2.2.1), one needs to look for long codes. Given a fixed finite field $\mathbb{F}_q$ and a code over a variety X with $\dim X \geq 2$, one way to increase the length (the number of $\mathbb{F}_q$ rational points) is by blowing up points. The problem becomes finding divisors on each variety that satisfy theorem 3.2.5.

4.2 Naive Construction on Surfaces

Here we attempt to take a code on a smooth projective surface X, and by blowing up points and lifting certain divisors, create longer codes on surfaces. First we review the intersection theory on surfaces.

4.2.1 Intersection Theory of Blow-Ups of Points on Surfaces

If $\pi : \tilde{X} \to X$ is a blowup of a surface at points P_i, $i = 1, \ldots, t$, with exceptional divisors E_i above each P_i, then $\operatorname{Pic} \tilde{X} \cong \operatorname{Pic} X \oplus \mathbb{Z}^t$, with each $\mathbb{Z}$ generated by an exceptional divisor E_i. $\operatorname{Pic} \tilde{X}$ has intersection calculus $C, D \in \operatorname{Pic} X \Rightarrow \pi^* C.\pi^* D = C.D$, $(\pi^* C).E_i = 0$, $E_i^2 = -1$, $E_i.E_j = 0$ for $i \neq j$ [22, Ch V, Prop 3.2].

4.2.2 An Attempt at a Family of Codes

Now let $\cdots \to X_i \to X_{i-1} \to \cdots \to X_1 \to X_0$ be a sequence of smooth surfaces defined over $\mathbb{F}_q$, with $\pi_i : X_{i+1} \to X_i$ the blowup of t_i $\mathbb{F}_q$-rational points on X_i ($t_i > 0$), which we can specify later. Subscripts on symbols in this chapter will associate those

symbols with the surface X_i or with the code on X_i. X_i has $n_i = \#X_i(\mathbb{F}_q)$ rational points. Assume $n_i > 0$ for all i. Let E_i^k be the set of exceptional divisors from the blowup π_i, with index $k = 1, 2, \ldots, t_i$. Blowing up $t_i > 0$ points on surface X_i, we obtain $q + 1$ points over each blown up point, thus $n_{i+1} = n_i + t_i(q + 1)$.

We then want to use theorem 3.2.5 to construct codes on each X_i, so we start by covering each with curves. Cover the n_0 $\mathbb{F}_q$ rational points on X_0 with curves $C_0^1, C_0^2, \ldots, C_0^{s_0}$. To cover all the rational points on each X_i, define curves iteratively as follows. The $\mathbb{F}_q$ rational points of surface X_i will be covered by s_i curves. Assume of the t_i points blown up by π_i that λ_i^j of them lie on curve C_i^j. $\sum_j \lambda_i^j \geq t_i$ (blowing up an intersection of two curves causes the inequality). Define, for $j = 1, 2, \ldots, s_i$, curves $C_{i+1}^j = \pi_i^* C_i^j - \sum E_i^\beta$, where the sum is over the λ_i^j exceptional divisors lying over points blown up on C_i^j (that is, C_{i+1}^j is the strict transform of C_i^j). Add the exceptional divisors as additional curves to cover X_{i+1}, giving more curves $C_{i+1}^j = E_i^k$ for enough $j = s_i + 1, \ldots, s_{i+1}$ and k chosen uniquely until all E_i^k are chosen. $s_{i+1} = s_i + t_i$. Thus at step i the curves are (iterated) strict transforms of an original curve C_0^j on X_0, or come from iterated strict transforms from some intermediate $E_{i_0}^j$ on X_{i_0}, or are exceptional divisors from the previous blow up. Note that any curve C_i^j thus has $q+1$ points if it comes from some E_i^j or has $\#C_0^j(\mathbb{F}_q)$ points if it comes from some C_0^j. To simplify notation, $C_{i+1}^j = C_i^j$ denotes the (iterated) strict transform when the subscripts differ.

Next give surface X_0 line bundles L_0 and H_0 satisfying theorem 3.2.5. We then need line bundles L_i and H_i on X_i satisfying the conditions 4.1, 4.2, 4.3, and 4.4 from theorem 3.2.5. From looking at divisors on X_i and X_{i+1}, and using the intersection calculus in section 4.2.1, one method to get such line bundles is to define line bundles on X_{i+1}, using H_i and L_i from X_i, by $H_{i+i} = h\pi_i^* H_i - \sum_j E_i^j$ and $L_{i+1} = h\pi_i^* L_i - \sum_j E_i^j$, for some integer $h > 0$ to be determined below. Note that H_i nef implies H_{i+1} is nef.

For the rest of the code parameters, use theorem 3.2.5. The dimension of the code on X_i is $k_i = h^0(X_i, L_i)$. Set $m_i = \sum_{j=0}^{j=s_i} L_i.C_i^j$. $L_i.C_i^j \geq 0$ implies $m_i \geq 0$. The distance of the code on X_i is $d_i \geq n_i - m_i$ if $n_i > m_i$.

Finally, in order to obtain codes on X_i, from theorem 3.2.5 we require for all i and j

$$H_i.C_i^j > 0 \tag{4.1}$$

$$L_i.C_i^j \geq 0 \tag{4.2}$$

$$C_i^j.H_i > L_i.H_i \tag{4.3}$$

$$n_i > m_i \geq 0 \tag{4.4}$$

We then have using the calculus in section 4.2.1

$$H_{i+1}.C_{i+1}^j = \begin{cases} (h\pi_i^* H_i - \sum_k E_i^k).(\pi_i^* C_i^j - \sum_\beta E_k^\beta) & : \quad C_{i+1}^j = C_i^j \\ (h\pi_i^* H_i - \sum_k E_i^k).(E_i^\beta) & : \quad C_{i+1}^j = E_i^\beta \end{cases}$$

Simplifying,

$$H_{i+1}.C_{i+1}^j = \begin{cases} hH_i.C_i^j - \lambda_i^j & : \quad C_{i+1}^j = C_i^j \\ 1 & : \quad C_{i+1}^j = E_i^\beta \end{cases} \tag{4.5}$$

Similarly,

$$L_{i+1}.C_{i+1}^j = \begin{cases} hL_i.C_i^j - \lambda_i^j & : \quad C_{i+1}^j = C_i^j \\ 1 & : \quad C_{i+1}^j = E_i^\beta \end{cases} \tag{4.6}$$

$$\begin{aligned} H_{i+1}.L_{i+1} &= (h\pi_i^* H_i - \sum_j E_i^j).(h\pi_i^* L_i - \sum_j E_i^j) && (4.7) \\ &= h^2 H_i.L_i - t_i && (4.8) \end{aligned}$$

Given a code on X_0 so that conditions 4.1, 4.2, 4.3, and 4.4 are met for $i = 0$ and all j, induct to find conditions meeting them for all i and j. Assume all four conditions are met for $i-1$ and for all j. Condition 4.1 succeeds in the case 4.5 gives $H_i.C_i = 1$ or $H_i.C_i = hH_{i-1}.C_{i-1} - \lambda_{i-1}^j > 0$. Since $H_{i-1}.C_{i-1}$ is assumed positive, and can be as small as 1, this requires $h > \lambda_j^{i-1}$, for all $i-1$ and j. In particular,

E_{i-1}^j has $q+1$ points, forcing $h > q+1$. This condition also suffices to ensure 4.2 holds for all i and j, leaving 4.3 and 4.4.

To ensure condition 4.3, applying 4.8 to $H_i.L_i$ repeatedly gives (for $i > 0$)

$$H_i.L_i = h^{2i} H_0.L_0 - \sum_{j=0}^{i-1} (h^2)^{i-1-j} t_j \tag{4.9}$$

Substituting in condition 4.3 gives

$$H_i.C_i > h^{2i} \left(H_0.L_0 - \sum_{j=0}^{i-1} \frac{t_j}{(h^2)^{j+1}} \right) \tag{4.10}$$

Since the left hand side is positive and as small as 1, and both sides are integers, this relation is true for all i if and only if the right hand side is ≤ 0 for all $i > 0$. This is equivalent to

$$H_0.L_0 \leq \sum_{j=0}^{i-1} \frac{t_j}{(h^2)^{j+1}} \tag{4.11}$$

Since this must hold for all $i > 0$, a necessary and sufficient condition for 4.11 to be satisfied, and hence necessary and sufficient for 4.3 to be met, is that

$$H_0.L_0 \leq \frac{t_0}{h^2} \tag{4.12}$$

Computing $m_i = \sum_j L_i.C_i^j$ is a bit more work. To simplify the calculation, assume that no blown up point at any stage is an intersection of any curves; thus $\sum \lambda_k^j = t_k$. Using equation 4.6, in the case the C_i^j is the iterated transform of some C_0^j we have

$$L_i.C_i^j = h^i L_0.C_0 - \sum_{k=0}^{i-1} h^{i-1-k} \lambda_k^j$$

Summing over all s_0 such curves gives a contribution to m_i of

$$s_0 h^i L_0.C_0 - \sum_{k=0}^{i-1} h^{i-1-k} t_k$$

For those C_i^j coming from some E_k^j, $0 \leq k < i$ fixed, we get a contribution of

$$t_k \left(h^{i-k-1} - \frac{h^{i-k-1} - 1}{h - 1} \right)$$

Summing these we obtain for $i > 0$

$$m_i = h^i s_0 L_0.C_0 - t_0 \frac{h^i - 1}{h - 1} + \sum_{k=0}^{i-1} t_k \frac{h^{i-k} - 2h^{i-k-1} + 1}{h - 1} \tag{4.13}$$

This can be rewritten

$$m_i = \frac{h^i}{h-1} \left((h-1)s_0 L_0.C_0 + \left(1 - \frac{2}{h}\right) \sum_{k=0}^{i-1} \frac{t_k}{h^k} + \frac{1}{h^i} \sum_{k=0}^{i-1} t_k - t_0 \left(1 - \frac{1}{h^i}\right)\right) \tag{4.14}$$

The requirement is $0 \leq m_i < n_i = n_0 + (q+1) \sum_{k=0}^{i-1} t_k$ to obtain codes. However equation 4.14 is difficult to analyze, although it can be shown m_i grows on order $O(h^i)$. This means n_i must grow this fast or faster, which places some bounds on the average size of the t_k. Recall that $h > q + 1$. For example, if all $t_i = 1$, then $n_i = n_0 + (q+1)i$ is less than 4.14 for large i, so it is impossible always to take $t_i = 1$.

This is an area needing more analysis.

4.3 Conclusion

"Though this be madness, yet there is method in't." William Shakespeare (1564-1616)

Summarizing, necessary and sufficient restrictions on h to guarantee that conditions 4.1, 4.2, and 4.3 are met for all i and j are

$$\begin{array}{rcl} h & > & \max_j \{q+1, \lambda_0^j\} \\ \frac{t_0}{h^2} & \geq & H_0.L_0 \end{array} \tag{4.15}$$

Simple requirements ensuring condition 4.4 are not completely understood, further than equation 4.14 and $0 \leq m_i < n_i$. If these four criteria can be met for all i, then we have an infinite family of codes.

In order to make this into family of ***good*** codes, the asymptotic bounds on rates and relative distances are needed. Unfortunately, even in the simplest cases, evaluating the dimensions $k_i = h^0(X_i, L_i)$ seems quite hard. There might be some way to relate k_i to k_{i-1} and induct, but I could prove no such results. The analysis of the relative distance is also difficult, but seems more likely to be understood. Also, there are many variations on the above method, such as allowing varying values for h at

each blowup or changing the form of H_i and L_i. It seems that blowing up points to make good families of codes will be difficult in this generality.

Example 4.3.1 Let C be a smooth curve over $\mathbb{F}_q$ with γ rational points. Let $X_0 = C \times \mathbb{P}^1$ with $n_0 = (q+1)\gamma$ rational points over $\mathbb{F}_q$. Let C_0^j be copies of $\mathbb{P}^1$ for $j = 1, 2, \ldots, \gamma$, disjoint and covering $(q+1)\gamma$ of the points. Pic $X =$ Pic $C \oplus \mathbb{Z}$. Choose L_0 and H_0 ample so that $L_0.H_0 > 0$. Each C_0^i has $q+1$ points on it. To take the first step to X_1, there must be some number $t_0 \leq n_0$ of points to blow up large enough so there exists an integer h with $q+1 < h \leq \sqrt{t_0}/(L_0.H_0)$. It is sufficient to take $(q+2)(L_0.H_0) < \sqrt{t_0}$. This h meets the conditions in equation 4.15. But the conditions on m_i still need checked in order to continue constructing the family.

5. CODES FROM RULED SURFACES

5.1 Notation and Theory

Now specialize to the case of ruled surfaces following [22, V.2]. Fixing notation: C is a smooth curve of genus g defined over $\mathbb{F}_q$. $\mathcal{E}$ is a locally free sheaf of rank 2 over C, defined over $\mathbb{F}_q$, corresponding to a rank 2 vector bundle E.

Definitions 5.1.1

1. $\mathcal{E}$ is **decomposable** if $\mathcal{E} \cong \mathcal{L}_1 \oplus \mathcal{L}_2$ for invertible sheaves $\mathcal{L}_i$ on C

2. $\mathcal{E}$ is **normalized** if $H^0(\mathcal{E}) \neq 0$ but $H^0(\mathcal{E} \otimes \mathcal{L}) = 0$ for all invertible sheaves $\mathcal{L}$ on C with $\deg \mathcal{L} < 0$

3. If $\mathcal{E}$ is normalized define $e = -\deg \bigwedge^2 \mathcal{E}$

4. $X = \mathbb{P}(Symm(\mathcal{E}))$ is a ruled surface, equipped with $\pi : X \to C$, a $\mathbb{P}^1$ bundle with a section and a relatively ample line bundle $\mathcal{O}_X(1)$. Let C_0 be the corresponding divisor. $\mathcal{E}$ normalized implies C_0 is an image of a section of π

Assume $\mathcal{E}$ is normalized. If $\mathcal{E}$ is decomposable then $e \geq 0$. All such values of e are possible: for example taking $\mathcal{E} = \mathcal{O} \oplus \mathcal{O}(-e)$. If $\mathcal{E}$ is indecomposable then $-g \leq e \leq 2g-2$ [22, Theorem 2.12b,ex. 2.5]. When $\mathcal{E}$ is normalized, e is an invariant of the surface X.

Then we have the following facts from [22, V Proposition 2.9]; using the notation above:

Lemma 5.1.2 *Let f be a fiber of π.*

$\operatorname{Pic} X \cong \mathbf{Z} \oplus \pi^* \operatorname{Pic} C$ *where* $\mathbf{Z}$ *is generated by* C_0*.*

$\operatorname{Num} X \cong \mathbf{Z} \oplus \mathbf{Z}$, $C_0.f = 1$, $f^2 = 0$, $C_0^2 = -e$.

Let $D = aC_0 + bf$ be a divisor, $p =$ char $\mathbb{F}_q$. Define

$$\kappa = \begin{cases} e & e \geq 0 \\ \frac{1}{2}\, e & e < 0 \quad g < 2 \\ \frac{1}{2}\, e + \frac{g-1}{p} & e < 0 \quad g \geq 2 \end{cases}$$

Then *regarding the divisor $D = aC_0 + bf$: [22, V, Theorems 2.20-2.21 and exercise 2.14]*

If *$e \geq 0$ or $g \leq 1$* ***then*** *D is ample (nef) $\Leftrightarrow$ $a > 0$ and $b > a\kappa$ (resp. $a \geq 0$ and $b \geq a\kappa$).*

In positive characteristic, ***if*** *$e < 0$ and $g > 1$* ***then*** *D is ample (nef) $\Rightarrow$ $a > 0$ and $b > \frac{1}{2}ae$ (resp. $a \geq 0$ and $b \geq \frac{1}{2}a$). $a > 0$ and $b > a\kappa \Rightarrow D$ ample.*

If *$e \geq 0$ and $Y \not\equiv C_0$ is an irreducible curve on X with $Y \equiv D$* ***then*** *$a > 0$ and $b \geq a\kappa$.*

If *E is the direct sum of 2 ample line bundles on C* ***then*** *C_0 is ample [23, Theorem 3.1.1]*

Note 5.1.3 [21] had $\frac{p}{g-1}$ instead of the correct $\frac{g-1}{p}$ listed above.

Then the main result for ruled surfaces is [21, Theorem 5.29]:

Theorem 5.1.4 *Let C be a nonsingular curve of genus g, $\mathcal{E}$ a normalized vector bundle of rank 2 over C, and X the associated ruled surface $\pi : X = \mathbb{P}(S(\mathcal{E})) \to C$, with invariant $e \geq -g$. f is a fiber over a point $P_0 \in C$, and $\gamma = \#C(\mathbb{F}_q)$. Fix integers $a \geq 0$ and $b \geq 0$. If $\mathcal{E}$ is not ample set $l = a(\lceil k \rceil - e) + b \quad (= b$ if $e \geq 0)$, else $l = b - ae$.* ***If*** *$l < \gamma$ and the bound on d is positive,* ***then*** *there are $[n, k, d]$ codes with parameters:*

$$\begin{aligned} n &= (q+1)\,\gamma \\ k &= h^0(C, Symm^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)) \\ d &\geq n - (\gamma - l)a - (q+1)l \end{aligned}$$

Proof Let $f_1, f_2, \ldots, f_\gamma$ be the fibers over the $\mathbb{F}_q$ points of C. These disjoint lines contain all the $\mathbb{F}_q$-rational points of X, and are the curves C_i in theorem 3.2.1. Let $L \equiv aC_0 + bf$. [22, V, 2.1-4, and II, 7.11] $\Rightarrow$

$$\Gamma(X, L) \cong \Gamma(C, \pi_* L) \cong \Gamma(S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0))$$

Let $H = C_0 + \lceil\kappa\rceil f$. Then H is nef, $H.f_i = 1$, $L.f_i = a$ for all i, and

$$\begin{aligned} H.L &= aC_0^2 + (b + \lceil\kappa\rceil a)C_0.f + b\lceil\kappa\rceil f^2 \\ &= -ea + b + a\lceil\kappa\rceil \\ &= a(\lceil\kappa\rceil - e) + b \\ (&= b \text{ if } e \geq 0) \end{aligned}$$

By Theorem 3.2.5 and Corollary 3.2.3, $l \leq \frac{L.H}{\min\limits_i\{C_i.H\}} = \frac{a(\lceil\kappa\rceil - e)+b}{1} \Rightarrow$

$$l \leq a(\lceil\kappa\rceil - e) + b$$

$\mathcal{E}$ ample $\Rightarrow C_0$ nef, so let $H = C_0$, which gives $l = H.L = b - ae$. ■

Remark 5.1.5 [21, 5.29] omits *normalized* in the statement above, and states that if $\mathcal{E}$ is ample, then $l = b - e$, which is incorrect. See sections 5.2.2 and 5.1.6 for counterexamples if normalized is omitted. [21, 5.30] uses a non-normalized sheaf, and computes e, which is then not an invariant, and is not guaranteed to satisfy $e \geq -g$. [21] does not clearly define e to be the invariant, and seems to treat it both ways. For example:

Counterexample 5.1.6 Over $\mathbb{P}^1$, which has genus 0, the non-normalized sheaf $\mathcal{E} = \mathcal{O}(1) \oplus \mathcal{O}(1)$ has deg $\bigwedge^2 \mathcal{E} = -2$ which violates $e \geq -g$.

5.2 Ruled Surfaces over P^1

First we classify codes on ruled surfaces over the unique genus 0 curve, $\mathbb{P}^1$, using theorem 5.1.4.

5.2.1 Codes

All indecomposable vector bundles over $\mathbb{P}^1$ are trivial [18]. Pic $\mathbb{P}^1 \cong \mathbb{Z}$, generated by a hyperplane section. Thus $\mathcal{E} \cong \mathcal{O}(t) \oplus \mathcal{O}(u)$ for some integers t and u, where $\mathcal{O} = \mathcal{O}_{\mathbb{P}^1}$. Since $\mathbb{P}(S(\mathcal{E})) \cong \mathbb{P}(S(\mathcal{E} \otimes \mathcal{O}(n)))$ for any integer n [22, II.7, ex 7.9b], reduce

to the normalized, decomposable case with $\mathcal{E} \cong \mathcal{O} \oplus \mathcal{O}(-e)$ for some integer $e \geq 0$. Then $\mathcal{E}$ is not ample, so $l = b$ in 5.1.4. All possible codes using this construction on ruled surfaces over $\mathbb{P}^1$ have the following parameters in the notation of theorem 5.1.4 (corresponding to a divisor $D \sim aC_0 + bf$ on X):

$$\begin{aligned} \gamma &= q + 1 \\ n &= (q+1)^2 \\ k &= h^0(\mathbb{P}^1, S^a(\mathcal{E}) \otimes \mathcal{O}(bP_0)) \\ d &\geq (q+1)^2 - (q+1-b)a - b(q+1) \end{aligned}$$

We require $b < \gamma = q + 1$ from theorem 5.1.4.

The bound on d is required to be positive to ensure the germ map α is injective, so we simplify the distance bound:

$$d \geq (q + 1 - a)(q + 1 - b)$$

Note this does not depend on the choice of e. Since $b < q+1$, requiring $(q+1-a)(q+1-b) > 0$ is equivalent to requiring $a < q + 1$. So for a given q and e combination, there are $(q + 1)^2$ codes under this construction, corresponding to $0 \leq a, b < q + 1$.

To compute the dimension k, note that $S^a(\mathcal{E}) \otimes \mathcal{O}(bP_0) \cong \bigoplus_{j=0}^{j=a} \mathcal{O}(b - je)$. Over $\mathbb{P}^1$, since cohomology commutes with direct sums, Riemann-Roch gives the dimension $k = \sum(b - je + 1)$, where the sum is over nonnegative j such that $je \leq b$ and $j \leq a$. So we see that the dimension of the code can be increased by increasing either a or b. However, as usual in coding theory, this decreases the distance d of the code.

To evaluate the performance of these codes, notice that increasing e decreases the dimension k of the code, and leaves the distance d unchanged, so taking $e = 0$ will result in the largest dimension k for fixed a, b. Then we have $k = \sum_{j=0}^{j=a}(b + 1) = (a + 1)(b + 1)$. This gives

Theorem 5.2.1 (Lomont Code #1) *The construction of Theorem 5.1.4 applied to ruled surfaces over $\mathbb{P}^1$, defined over the finite field $\mathbb{F}_q$, results in $[n,k,d]$ codes with parameters*

$$\begin{aligned} n &= (q+1)^2 \\ k &= \sum (b - je + 1) \\ d &\geq (q+1-a)(q+1-b) \end{aligned}$$

where the sum is over nonnegative j so that $je \leq b$ and $j \leq a$, and $0 \leq a, b < q+1$, $0 \leq e$.

The codes with highest rates are then when $e = 0$, giving codes for integers $0 \leq a, b < q+1$

$$\begin{aligned} n &= (q+1)^2 \\ k &= (a+1)(b+1) \\ d &\geq (q+1-a)(q+1-b) \end{aligned} \tag{5.1}$$

In this case $X \cong \mathbb{P}^1 \times \mathbb{P}^1$.

Proof Shown above. ∎

As a sanity check compare this to the Singleton Bound (see equation 2.1), $n+1 \geq k+d$. Theorem 5.2.1 gives

$$\begin{aligned} (q+1)^2 + 1 &\geq (a+1)(b+1) + (q+1-a)(q+1-b) \\ 1 &\geq (a+1)(b+1) - (a+b)(q+1) + ab \\ 1 &\geq 2ab - q(a+b) \end{aligned}$$

and it can be shown that for $0 \leq a, b \leq q$ this is always satisfied.

Note 5.2.2 (Decoding) The Lomont code #1 has parameters which look like a product code. There is a way to define a Goppa code over $\mathbb{P}^1$ so it has $q+1$ points by taking the poles at a point not defined over $\mathbb{F}_q$. Then the decoding algorithms for the Goppa code [40] should be able to decode the Lomont code #1 as a product code. This needs checked.

5.2.2 Comparison to Product Codes

The Reed Solomon (RS) codes over $\mathbb{F}_q$ have parameters $[q-1, k, q-k]$ for $0 \leq k \leq q-1$ [43, Ch 8.2]. So the Lomont Code #1 in theorem 5.2.1 is longer than the product code (section 2.3) from two RS codes, which has parameters $[(q-1)^2, ab, (q-a)(q-b)]$, $0 \leq a, b \leq q-1$. For comparison, fix the field to be the commonly used field $\mathbb{F}_{256}$, and compare the best relative distance δ for a desired rate r (see Table 5.1). The leftmost column is the desired rate $r = 0.1, 0.2, \ldots, 0.9$. Then all legal combinations of a and b are searched to find the best performing δ when the corresponding rate is $\geq r$. The left block shows the optimal choices of a and b giving the rate and δ combination for the Reed Solomon code, and the right block shows the same information for the Lomont Code #1. For example, looking for a code with rate at least 0.8, the highest δ product RS code is when $a = 228$, $b = 229$, and has relative distance $\delta = 0.1163$. The corresponding best Lomont code is when $a = b = 229$ and has $\delta = 0.1187$, so is a slightly better code. For this example the product code could correct 377 errors, but the Lomont code could correct 391 errors, and thus is slightly better at handling burst errors. So besides being longer than the RS product code, the Lomont code for this example has better relative distance. Note that the Lomont code is better for 6 of the 9 values tested.

A Counterexample

If we do not require $\mathcal{E}$ to be normalized we get impossible codes, showing that normalized is necessary in theorem 5.1.4. Let $\mathcal{F} = \mathcal{O}(t) \oplus \mathcal{O}(u)$ for an integers $t \geq u$. Then

$$S^a(\mathcal{F}) \otimes \mathcal{O}(bP_0) \cong \bigoplus_{j=0}^{j=a} \mathcal{O}((a-j)t + ju + b)$$

From Riemann-Roch the dimension $k = \sum at + j(u-t) + b + 1$, where the sum is over $0 \leq j \leq a$ and $at + j(u-t) + b \geq 0$. Letting $\mathcal{E}$ be the normalized vector bundle

Table 5.1
Comparison of the Reed Solomon code to the Lomont code #1

	Reed Solomon				Lomont Code #1			
rate	a	b	rate	δ	a	b	rate	δ
0.1	81	81	0.1009	0.470973	80	81	0.100562	0.47165
0.2	114	115	0.201615	0.307912	114	114	0.20023	0.309603
0.3	140	140	0.301423	0.206936	140	140	0.301004	0.207255
0.4	161	162	0.401107	0.137332	162	162	0.402262	0.136641
0.5	180	181	0.501038	0.0876586	181	181	0.501506	0.0874502
0.6	198	198	0.602907	0.0517339	198	199	0.602583	0.05181
0.7	213	214	0.700992	0.0277739	214	215	0.703114	0.0273433
0.8	228	229	0.802953	0.0116263	229	229	0.800921	0.01187
0.9	242	242	0.900638	0.00301423	243	243	0.901391	0.00296749

$\mathcal{F} \otimes \mathcal{O}(-t) \cong \mathcal{O} \oplus \mathcal{O}(u-t)$, we have that $e = -(u-t) = t-u \geq 0$. The length of the code is $n = (q+1)^2$, and these are the Lomont codes in theorem 5.2.1 above.

Counterexample 5.2.3 However, taking the unnormalized $\mathcal{F}$ with $t > 0$ and $u = -t$, since all terms in the dimension sum are nonnegative, we have that $k \geq at$. $e = 0$, and $\mathcal{F}$ is not ample, so $l = b$. The distance is again bounded by $d \geq (q+1)^2 - (q+1-b)a - b(q+1)$, which is independent of t. Taking $a = 1$, $b = 0$, then $d \geq (q+1)q$, so α is injective and we have a code. But letting t increase without bound increases k without bound, a contradiction since the unbounded k-dimensional vector space cannot be a subspace of the fixed n-dimensional one.

5.3 Decomposable Bundles over Positive Genus Curves

Let C be a curve of genus $g \geq 1$ over $\mathbb{F}_q$, and let $\mathcal{E} = \mathcal{O} \oplus \mathcal{O}(-e)$ for some nonnegative integer e, giving the resulting surface X an invariant of $e \geq 0$.

A bound on the number γ of $\mathbb{F}_q$-rational points on C is $|\gamma-(q+1)| \leq g\lfloor 2\sqrt{q}\rfloor$ [46], but can be improved in many cases, some of which are mentioned in chapter 6 which deals with explicit curves reaching known bounds. Following the reasoning from the genus 0 case, we get that

$$
\begin{aligned}
n &= \gamma(q+1) \\
d &\geq n-(\gamma-b)a-(q+1)b
\end{aligned}
$$

The dimension k is estimated using $S^a(\mathcal{E}) \otimes \mathcal{O}(bP_0) \cong \bigoplus_{j=0}^{j=a} \mathcal{O}(-je) \otimes \mathcal{O}(bP_0)$. Using Riemann-Roch, $l(D) = \deg D + 1 - g + l(K-D)$ gives that k is in the form $\sum(b-je) - g + 1 + \zeta$, where the sum is over certain nonnegative terms as usual, and ζ is also nonnegative from the $l(K-D)$ part of Riemann-Roch. Since the distance does not rely on e, we can maximize the dimension k by making $e=0$. This proves

Theorem 5.3.1 *Given a genus g smooth projective curve C over $\mathbb{F}_q$, and an integer $e \geq 0$. Let $\gamma = \#C(\mathbb{F}_q)$, $\mathcal{E} = \mathcal{O}_C \otimes \mathcal{O}_C(-e)$, and X be the corresponding ruled surface. For integers $0 \leq a$, $0 \leq b < \gamma$ there are codes (assuming the bound on d is positive)*

$$
\begin{aligned}
n &= \gamma(q+1) \\
k &= \sum(b-je) - g + 1 + \zeta_j \\
d &\geq (q+1-a)(\gamma-b)
\end{aligned}
$$

where the sum is over those j so that $0 \leq j \leq a$ and $je \leq b$. $\zeta_j = l(K-D_j)$, where K is the canonical divisor on C, and $D_j = \mathcal{O}(b-je)$. Again it is clear that $e=0$ gives the largest dimension, then $X \cong C \times \mathbb{P}^1$, and the best such codes are product codes.

Without specific curves, it is hard to go much further than this, since one needs information about the canonical divisor K and the dimensions ζ_j. An interesting case would be to study the curves of Garcia and Stichtenoth (see section 7.1), since they have many rational points and would result in very long codes.

5.4 Ruled Surfaces over Elliptic Curves

5.4.1 Vector Bundles over Elliptic Curves

Here recall some facts from the classification of indecomposable vector bundles over elliptic curves. The classification over algebraically closed fields of any characteristic was done by Atiyah in [3], and the extension to perfect fields was done in the thesis of Agnes Williams under G. Faltings, and was stated in a paper by Arason, Elman, and Jacob [2]. Thus the following also is true for the case we need, namely the finite field case $K = \mathbb{F}_q$.

The facts are for an arbitrary perfect field K and elliptic curve C defined over K:

1. To each K-rational point $P \in C$ there is constructed a vector bundle $E_{r,d}(P)$ of rank r and degree d on C.

2. Each $E_{r,d}(P)$ is shown to be absolutely indecomposable.

3. $E_{r,d}(P) \cong E_{r,d}(Q) \Rightarrow P = Q$

4. For an absolutely indecomposable vector bundle M of rank r and degree d on C there is found a rational point $P \in C$ such that $M \cong E_{r,d}(P)$.

5. There is an absolutely indecomposable vector bundle F_r of rank r and degree 0 on C, unique up to isomorphism, such that F_r has non-trivial global sections. Moreover, there is an exact sequence

$$0 \to \mathcal{O}_C \to F_r \to F_{r-1} \to 0$$

If M is an absolutely indecomposable vector bundle of rank r and degree d, then there is a line bundle L of degree 0 on C, unique up to isomorphism, such that $M \cong L \otimes F_r$. M contains L as a subbundle.

6. $\dim \Gamma(F_r \otimes F_s) = \min\{r, s\}$. Given a line bundle L, $\dim \Gamma(L \otimes F_r \otimes F_s) = 0$ unless $L \geq 1$ [3, III, Lemma 17].

7. $F_r \otimes F_s \cong \sum_{j=1}^{\min(r,s)} F_{r_j}$, $\sum_j r_j = rs$ [3, III, Lemma 18].

5.4.2 Codes

Let C be an elliptic curve over $\mathbb{F}_q$. Let $\mathcal{E}$ be a rank 2 normalized vector bundle over C defined over $\mathbb{F}_q$. The case $\mathcal{E}$ decomposable is covered by section 5.3. If $\mathcal{E}$ is indecomposable, then [22, V, Theorem 2.15] gives that $\deg \mathcal{E}$ is 0 or 1.

Using the decomposable case from section 5.3 would not be difficult to do for an elliptic curve, and would result in a product code from results in that section, so we do not do it here.

The Degree 0 Case

We associate the (torsion-free) coherent sheaf $\mathcal{F}_r$ to the vector bundle F_r. [45]. To compute the dimension of the codes in this case, we need to understand the structure of $S^n(\mathcal{F}_r)$, enough of which is given by following theorem for our purposes.

Theorem 5.4.1 *Denote by $\mathcal{F}_r$ the unique degree 0 rank r indecomposable vector bundle with a global section over the elliptic curve C, both defined over the perfect field K.* ***Then*** *$S^n(\mathcal{F}_r) \cong \oplus \mathcal{F}_{r_i}$, for some $\mathcal{F}_{r_i}$, with $\sum_i r_i = \binom{n+r-1}{r-1}$.*

Proof Write $\mathcal{F}$ for $\mathcal{F}_r$. Let $S^n(\mathcal{F}) \cong \oplus \mathcal{E}_i$, where the $\mathcal{E}_i$ are indecomposable. Let $\mathcal{L}$ be a degree 0 line bundle with no global section (e.g., corresponding to a divisor $P - Q$ for $P \neq Q$). In the exact sequence

$$0 \to \mathcal{I} \to \mathcal{F}^{\otimes n} \to S^n(\mathcal{F}) \to 0 \tag{5.2}$$

$\deg \mathcal{I} = 0$ since degree is additive, and the other two terms have degree 0 by theorems A.1.4 and A.1.6. After tensoring with $\mathcal{L}$, this gives the cohomology sequence

$$\begin{array}{ccccccccc} 0 & \to & H^0(\mathcal{I} \otimes \mathcal{L}) & \to & H^0(\mathcal{F}^{\otimes n} \otimes \mathcal{L}) & \to & H^0(S^n(\mathcal{F}) \otimes \mathcal{L}) & \to & \\ & & H^1(\mathcal{I} \otimes \mathcal{L}) & \to & H^1(\mathcal{F}^{\otimes n} \otimes \mathcal{L}) & \to & H^1(S^n(\mathcal{F}) \otimes \mathcal{L}) & \to & 0 \end{array} \tag{5.3}$$

The higher terms all vanish by Grothendieck Vanishing [22, III, Theorem 2.7].

Then using properties 6 and 7 in section 5.4.1, and that for any vector bundle $\mathcal{E}$ Riemann-Roch gives $h^0(\mathcal{E}) - h^1(\mathcal{E}) = \deg \mathcal{E}$, we get that both terms involving $\mathcal{F}^{\otimes n} \otimes \mathcal{L}$

vanish. Thus $H^0(\mathcal{I} \otimes \mathcal{L}) = 0$, so using Riemann-Roch again gives $H^1(\mathcal{I} \otimes \mathcal{L}) = 0$, which implies $H^0(S^n(\mathcal{F}) \otimes \mathcal{L}) = 0$. So $\deg \mathcal{E}_i \leq 0$ for every i. Since degree is additive over direct sums [22, II, ex 6.12(3)] it must be that $\deg \mathcal{E}_i = 0$ for every i.

From Property 5, section 5.4.1, $\mathcal{E}_i \cong \mathcal{F}_{r_i} \otimes \mathcal{L}_i$ for some degree 0 invertible sheaves $\mathcal{L}_i$. Suppose some $\mathcal{L}_i \ncong \mathcal{O}_C$. Then taking the sequence 5.2 and tensoring with $\mathcal{L}_i^{-1}$, we get the cohomology sequence

$$\begin{array}{cccccccc} 0 & \to & H^0(\mathcal{I} \otimes \mathcal{L}_i^{-1}) & \to & H^0(\mathcal{F}^{\otimes n} \otimes \mathcal{L}_i^{-1}) & \to & H^0(S^n(\mathcal{F}) \otimes \mathcal{L}_i^{-1}) & \to \\ & & H^1(\mathcal{I} \otimes \mathcal{L}_i^{-1}) & \to & H^1(\mathcal{F}^{\otimes n} \otimes \mathcal{L}_i^{-1}) & \to & H^1(S^n(\mathcal{F}) \otimes \mathcal{L}_i^{-1}) & \to & 0 \end{array}$$

Again by the reasoning above, the terms involving $\mathcal{F}^{\otimes n}$ vanish, causing the terms involving $\mathcal{I}$ to vanish, so again $H^0(S^n(\mathcal{F}) \otimes \mathcal{L}_i^{-1}) = 0$. But $S^n(\mathcal{F}) \otimes \mathcal{L}_i^{-1}$ has $\mathcal{F}_{r_i}$ as a direct summand, and thus has a global section, a contradiction. So all $\mathcal{L}_i \cong \mathcal{O}_{\mathcal{C}}$, giving that $S^n(\mathcal{F}_r) \cong \oplus_{i=1}^m \mathcal{F}_{r_i}$.

The rank of the left hand side is given in the appendix, theorem A.1.5, so the right hand side, being additive, gives $\sum_i r_i = \binom{n+r-1}{r-1}$. ■

Note 5.4.2 In special cases we can find precisely which $\mathcal{F}_{r_i}$ occur. For example, using [3] and the techniques above, $S^2(\mathcal{F}_2)$ can be found for any characteristic by examining possible ranks r_i, and counting global sections.

Now we can compute the parameters of codes arising from $\mathcal{F}_2$. Using theorem 5.1.4 we obtain

Theorem 5.4.3 (Lomont Code #2) *Let C be an elliptic curve with γ $\mathbb{F}_q$ rational points, $\gamma > 0$. Let a, b be integers with $0 < b < \gamma$, $0 \leq a < q + 1$.* ***Then*** *there are $[n, k, d]$ codes with*

$$n = (q+1)\,\gamma$$
$$k = (a+1)b$$
$$d \geq (q+1-a)(\gamma - b)$$

Remark 5.4.4 For $b = 0$ there is still a code, but the exact dimension is slightly more complex to compute, and appears to be uninteresting.

Proof We use theorem 5.1.4, in the case $\mathcal{E}$ is the unique indecomposable rank 2 degree 0 vector bundle over C with a global section. The value for n follows immediately. $\mathcal{E}$ is not ample [24, Theorem 1.3], giving invariant $e = 0$, so $l = b$ in 5.1.4. The dimension arises from using theorem 5.4.1, Riemann Roch 2.4.1, and theorem A.1.4 in 5.1.4 to obtain:

$$\begin{aligned} k &= h^0(C, S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0)) \\ &= h^0(C, \oplus_i(\mathcal{F}_{r_i} \otimes \mathcal{O}_C(bP_0))) \\ &= \textstyle\sum_i h^0(C, \mathcal{F}_{r_i} \otimes \mathcal{O}_C(bP_0))) \\ &= \textstyle\sum_i r_i b \\ &= \tbinom{a+2-1}{2-1} b \\ &= (a+1)b \end{aligned}$$

Note that the bound on d positive if and only if $a < \frac{n-(q+1)b}{\gamma-b} = q+1$, so by theorem 5.1.4 we have a code. ■

Note 5.4.5 (Decoding) Similar to note 5.2.2, the Lomont code #2 has parameters which look like a product code. The methods of decoding mentioned there should also be able to decode the Lomont code #2. This too needs checked.

Theorem 5.4.6 (Lomont code #2 Rate) *Use the notation of theorem 5.4.3. For a fixed relative distance $\delta = \frac{d}{n}$, set $b_0 = \gamma\left(1 - \sqrt{\frac{(q+1)\delta}{(q+2)}}\right)$, and then $a_0 = \frac{(q+1)(\gamma\delta-\gamma+b_0)}{b_0-\gamma}$. This code has the highest rate $R = \frac{k}{n}$ when the integers (a, b) are one of the integer lattice points points $(\lfloor a_0 \rfloor, \lfloor b_0 \rfloor)$, $(\lceil a_0 \rceil, \lfloor b_0 \rfloor)$, or $(\lfloor a_0 \rfloor, \lceil b_0 \rceil)$, depending on which ones satisfy the requirement of the size of δ.*

Proof Given a fixed value for $\delta = \frac{d}{n}$, we wish find the values of a and b giving the highest rate $R = \frac{k}{n}$, treating a and b as real numbers. Assume $0 < b < \gamma$ and $0 < a < q+1$. Then

$$\begin{aligned} \delta &= \frac{(q+1)\gamma-(\gamma-b)a-(q+1)b}{(q+1)\gamma} \\ R &= \frac{(a+1)b}{(q+1)\gamma} \end{aligned}$$

Solving the first equation for a, and substituting into the second,

$$\begin{aligned} a &= \frac{(q+1)(\gamma\delta-\gamma+b)}{b-\gamma} \\ R &= \frac{b}{(q+1)\gamma}\left(1 + \frac{(q+1)(\gamma\delta-\gamma+b)}{b-\gamma}\right) \end{aligned}$$

which is valid for $0 < b < \gamma$. The first two derivatives of R with respect to b are

$$\begin{aligned} R' &= \tfrac{1}{\gamma(q+1)} + \tfrac{b^2-2\gamma b+(\delta-1)\gamma^2}{(b-\gamma)^2\gamma} \\ R'' &= \tfrac{2\gamma\delta}{(b-\gamma)^3} \end{aligned}$$

$b < \gamma \Rightarrow R'' < 0$, so roots of R' give local maxima. These roots occur when

$$b_0 = \gamma\left(1 \pm \sqrt{\frac{(q+1)\delta}{(q+2)}}\right)$$

$b < \gamma$ forces choosing the negative sign in the $\pm$, then this gives the best possible value of b_0 in the theorem. Then a_0 follows. Since R is concave downward, the best possible integer b for any given a must be $\lfloor b_0 \rfloor$ or $\lceil b_0 \rceil$. Similarly for a compared to a_0. Since (a, b) must be integers, and δ decreases as a or b increases, the combination $(\lceil a_0 \rceil, \lceil b_0 \rceil)$ will have too small a delta value, giving the other three combinations as possible outcomes. It is possible to construct examples with each combination as the best choice. ■

5.4.3 Comparison to Product Codes

Next we compare these codes with the product codes obtained from Goppa codes on C with Reed-Solomon codes on $\mathbb{P}^1$. On $\mathbb{P}^1$ over $\mathbb{F}_q$ the RS codes have parameters $[q-1, k_1, q-k_1]$ for $0 \leq k_1 \leq q-1$. The Goppa codes on C have parameters $[\gamma-1, k_2, \gamma-1-k_2]$ with $0 < k_2 < \gamma-1$. Similar to the above, for $0 < k_2 < \gamma-1$ and $0 \leq k_1 \leq q-1$ we have product code parameters

$$\begin{aligned} \delta_1 &= \tfrac{(\gamma-1-k_2)(q-k_1)}{(q-1)(\gamma-1)} \\ R_1 &= \tfrac{k_1 k_2}{(q-1)(\gamma-1)} \end{aligned}$$

Solving the first for k_1 and substituting into R_1 gives

$$R_1 = \frac{qk_2}{(q-1)(\gamma-1)} - \frac{k_2\delta_1}{\gamma-1-k_2}$$

The best possible value for k_2 then becomes, for a fixed δ_1,

$$k_2 = (\gamma-1)\left(1 \pm \sqrt{\frac{(q-1)\delta_1 - 1}{q}}\right)$$

We need $k_2 < \gamma - 1$, so we take the negative sign choice.

Using the same value for δ, substitute the best values to maximize the rates for each code, and subtract the resulting optimal rates, giving the difference between the optimal rates as a function of q and δ.

$$err(q, \delta) = R - R_1 = -\frac{2}{q^2 - 1} + 2\sqrt{\delta}\left(\sqrt{\frac{q}{q-1}} - \sqrt{\frac{q+2}{q+1}}\right) \tag{5.4}$$

Over a field size used often in practice, $q = 256$, this simplifies to $err(256, \delta) = -0.000030518 + 0.0000304586\sqrt{\delta}$. Since $\delta \in [0, 1]$, this shows the surface code has a slightly lower rate than the product code. Below in section 5.4.3 this is shown to be true for any size finite field. The two rates converge to the same value as q gets larger and larger, so for large fields the Lomont code #2 code performs arbitrarily close to the product code from the RS code and Goppa code.

An Example

However, since the parameters a, b, k_1, and k_2 are restricted to integral values, sometimes the Lomont code #2 is slightly better than the product codes, since the rates are so close when considered as continuous functions. For example, see table 5.2. Here the field is fixed at $\mathbb{F}_{256}$ as in the genus 0 case, and the elliptic curve is $y^2 = x^3 + x + 1$, which has $\gamma = 255$ rational points. The left column is the desired rate $R = 0.1, 0.2, \ldots, 0.9$, and the rest shows the best parameters for the product code and the Lomont code #2. Notice in some cases, like the $R = 0.6$ case, that the Lomont code #2 has higher relative distance than the corresponding product code, but a lower rate. As in the genus 0 case, since it is longer but with a similar rate and relative distance, the Lomont code can correct longer burst errors than the product code can. For this example, the Lomont code #2 can correct 1694 errors, while the product code can correct 1659 errors.

Table 5.2
Comparison of the product code to the Lomont code #2

	Reed Solomon × Goppa				Lomont Code #1			
rate	k_1	k_2	rate	δ	a	b	rate	δ
0.1	81	80	0.100046	0.470125	81	80	0.100099	0.469978
0.2	115	113	0.200633	0.306948	115	113	0.200015	0.307683
0.3	140	139	0.300448	0.205960	141	139	0.301183	0.205325
0.4	162	160	0.400185	0.136421	162	161	0.400443	0.136263
0.5	181	179	0.500216	0.086846	182	180	0.502632	0.085832
0.6	198	197	0.602223	0.051042	199	197	0.601205	0.051331
0.7	214	212	0.700448	0.027235	215	213	0.702037	0.026917
0.8	229	227	0.802578	0.011255	229	228	0.800183	0.011536
0.9	242	241	0.900448	0.002810	243	242	0.901015	0.002777

Optimal Rate Comparison

To show $err(q,\delta) < 0$ for all $q > 1$ and $\delta \in [0,1]$, notice that

$$\begin{aligned} q^2 + q &> q^2 + q - 2 \\ q(q+1) &> (q+2)(q-1) \\ \tfrac{q}{q-1} &> \tfrac{q+2}{q+1} \\ \sqrt{\tfrac{q}{q-1}} &> \sqrt{\tfrac{q+2}{q+1}} \end{aligned}$$

Thus the coefficient of δ in $err(q,\delta)$ 5.4 is always positive, so to find the maximum of $err(q,\delta)$, we can assume $\delta = 1$. Assuming $q > 1$, if $err(q,1) < 0$ then

$$-\tfrac{2}{q^2-1} + 2\left(\sqrt{\tfrac{q}{q-1}} - \sqrt{\tfrac{q+2}{q+1}}\right) \quad < \quad 0$$

Multiply each side by $\sqrt{(q-1)/q}(q+1)/2 > 0$, obtaining

$$\begin{aligned}
-\frac{1}{\sqrt{(q-1)q}} + 1 + q - \sqrt{\frac{(q-1)(q+1)(q+2)}{q}} &< 0 \\
\left(1 + q - \frac{1}{\sqrt{(q-1)q}}\right)^2 &< \left(\sqrt{\frac{(q-1)(q+1)(q+2)}{q}}\right)^2 \\
1 - q - q^2 + q^3 + q^4 - 2\sqrt{(q-1)q}(q+1) &< 2 - q - 3q^2 + q^3 + q^4 \\
(2q^2-1)^2 &< \left(2\sqrt{(q-1)q}(q+1)\right)^2 \\
1 + 4q &< 4q^3
\end{aligned}$$

which always holds for $q > 1$. The steps are reversible, proving the optimal rate of the product code is slightly larger than the optimal rate of the Lomont code #2.

The Degree 1 Case

I have been unable to complete the analysis in this case. The trouble is computing $k = h^0(C, S^a(\mathcal{E}) \otimes \mathcal{O}(bP_0))$, for $\mathcal{E}$ a rank 2, degree 1, indecomposable vector bundle on the elliptic curve C. The problem is decomposing $S^a(\mathcal{E})$ in a manner similar to theorem 5.4.1. From the methods in the classification this should be possible, but I have been unable to solve it.

5.5 Conclusion

The codes in this chapter are comparable in performance to product codes. Over the elliptic curves, since the degree 0 case was comparable to the product codes, perhaps the degree 1 case will be as good or better than the product codes. It would be an interesting and worthwhile problem to finish this classification, and see if there is any improvement.

6. NEW CURVES OVER P^2

This chapter is a paper that will be published in *Experimental Mathematics.*

Yet More Projective Curves Over $\mathbb{F}_2$

Abstract All plane curves of degree less than 7 with coefficients in $\mathbb{F}_2$ are examined for curves with a large number of $\mathbb{F}_q$ rational points on their smooth model, for $q = 2^m, m = 3, 4, \ldots, 11$. Known lower bounds are improved, and new curves are found meeting or close to Serre's, Lauter's, and Ihara's upper bounds for the maximal number of $\mathbb{F}_q$ rational points on a curve of genus g.

6.1 Introduction

Let $\mathbb{F}_q$ denote the finite field with q elements. All absolutely irreducible homogeneous polynomials $f \in \mathbb{F}_2[x, y, z]$ of degree less than 7 are examined for those with a large number of $\mathbb{F}_q$ rational points, $q = 2^m, m = 3, 4, 5, \ldots, 11$, extending the results in [36]. A brute force search obtained all rational points for each polynomial of a given degree. The resulting list of polynomials with many rational points, perhaps with singularities, were then studied to determine if resolving singularities would add more rational points on the smooth model. The result is an exhaustive search of all curves resulting from desingularizing a homogeneous polynomial of degree less than 7 in $\mathbb{F}_2[x, y, z]$.

The rest of the paper is laid out as follows: first known bounds on the maximal number of $\mathbb{F}_q$ rational points of a genus g curve are recalled, along with some theorems that speed up the computations. Then the computation is described in some detail. A listing of the best found polynomials is given for each genus, allowing checking (by computer unless one has a lot of time!) the claimed number of rational points on

each curve. Finally the new lower bounds are listed in a table for each $\mathbb{F}_q$ and genus combination.

6.2 Genus Bounds and Irreducibility Tests

Let $f \in \mathbb{F}_2[x, y, z]$ be an absolutely irreducible homogeneous polynomial; f defines a projective plane curve C. Let $\tilde{C}$ be the smooth model, and g its genus. Some bounds on the genus can be deduced from knowing the number of $\mathbb{F}_q$ rational points in the plane and the number of singularities in the plane. $N_q(g)$ is the maximum number of $\mathbb{F}_q$-rational points on a smooth curve of genus g over $\mathbb{F}_q$. Serre's bound [46] on $N_q(g)$ is

$$|N_q(g) - (q + 1)| \leq g\lfloor 2\sqrt{q} \rfloor$$

where $\lfloor \alpha \rfloor$ is the integral part of α. This gives

$$N_q(g) \leq (q + 1) + g\lfloor 2\sqrt{q} \rfloor$$

so if there is an integer g_0 such that

$$q + 1 + g_0\lfloor 2\sqrt{q} \rfloor < p$$

where p is the point count on the particular curve C in question, then $g_0 < g$. If the number of singularities is r, and the degree of the polynomial f is d, then

$$g \leq \frac{(d - 1)(d - 2)}{2} - r$$

To get an estimate of the total number of points possible on the smooth model $\tilde{C}$ resulting from blowing up singularities the following estimate was used.

Theorem 6.2.1 *Let $C \subseteq \mathbb{P}^2$ be a plane curve of degree d with singularities $P_1, P_2, \ldots, P_r$, with multiplicities $m_1, m_2, \ldots, m_r$, for $r \geq 2$.* ***Then*** *$\sum_{i=1}^{r} m_i \leq \lfloor \frac{d}{2} \rfloor r + 1$ if d is odd, and $\sum_{i=1}^{r} m_i \leq \lfloor \frac{d}{2} \rfloor r$ if d is even.*

So the number of points obtained from blowing up singularities is bounded above by $\lfloor \frac{d}{2} \rfloor r + 1$.

Proof By Bezout's theorem, a line through any 2 singularities P_i and P_j implies $m_i + m_j \leq d$. Thus at most one singularity can have multiplicity $> d/2$, and the result follows. ■

More details on resolution of curve singularities can be found in [22] and [52].

To test for absolute irreducibility the following was used [41]:

Definition 6.2.2 *Let k be a field. The polynomial $f \in k[x_1, x_2, \ldots, x_n]$ has a* **simple solution** *at a point $P \in k^n$ if $f \in I(P) \setminus I(P)^2$, with $I(P)$ being the ideal of polynomials vanishing at P.*

Theorem 6.2.3 ***If*** *$f \in k[x_1, x_2, \ldots, x_n]$ is irreducible over the perfect field k and has a simple solution in k^n,* ***then*** *f is absolutely irreducible.*

Proof Since f is irreducible over k, its absolutely irreducible factors are conjugate over k. If $P \in k^n$ is a root of one of the factors, it must be a root of the others. But P only vanishes to order 1, thus f has one factor, and is absolutely irreducible. ■

The number of $\mathbb{F}_q$ points on a plane curve can be computed directly by brute force, as can lower bounds on the number of singularities, and then the above inequalities can be used to obtain bounds on the genus. So given a polynomial f, the number of rational points computed on it, and the number of singularities found, upper and lower bounds on the possible genus are obtained, which speeds up the search by removing curves early in the computation that have uninteresting combinations of genus and rational point count.

6.3 Computation

6.3.1 Storing Polynomials Compactly

All $\mathbb{F}_q$ rational points were found on each homogeneous polynomial of degree ≤ 5 in $\mathbb{F}_2[x, y, z]$, for $q = 2^m, m = 3, 4, \ldots, 11$. Due to the the time required, degree 6 homogeneous polynomials were examined only for $m = 3, 4, \ldots, 9$.

The most time consuming part was counting the number of $\mathbb{F}_q$-rational points on each plane curve. This was done with a C program using exhaustive search. Several ideas were used to reduce the complexity at each stage. Degree 6 computations will be described; the other degrees are similar. The code was checked for correctness by comparing the degree ≤ 5 results with [36], and in the process a few curves were found that were previously overlooked.

First, each homogeneous polynomial can be represented uniquely by a 32 bit integer, using each bit to signify the presence of a certain monomial in the polynomial. In degree 6, there are $\binom{6+2}{2} = 28$ different monomials of the form $x^i y^j z^k$ with $i+j+k = 6$ and $0 \leq i, j, k$. Each bit from 0 to 27 denotes the presence of a monomial, and the mapping $\alpha : \{\textit{homogeneous degree } 6\ f \in \mathbb{F}_2[x, y, z]\} \to \{1, 2, \ldots, 2^{28} - 1\}$ thus defined is a bijection. Thus each homogeneous polynomial $f \in \mathbb{F}_2[x, y, z]$ of degree 6 corresponds to a unique integer between 1 and $2^{28} - 1 \approx 268$ million.

6.3.2 Reducing Computation Time

To reduce the number of polynomials searched, equivalent ones under the action of $GL_3(\mathbb{F}_2)$ on the variables x, y, z were removed. To fit the entire degree 6 computation in memory, a bit table of 32 megabytes of RAM was used, with the position of each bit representing the number of a polynomial using the above bijection. All bits were set to 1, denoting all polynomials are still in the search space. Then the orbit of each polynomial under $GL_3(\mathbb{F}_2)$ was removed from the bit table, and the polynomial in each orbit requiring the least computation to evaluate was written to a data file. Since the size of $GL_3(\mathbb{F}_2)$ is 168, this was expected to give approximately a 168 fold decrease in the number of curves needing to be searched (not exactly 168 since some polynomials are invariant under some automorphisms). By using the representative of each orbit requiring the least work to evaluate, the search time was reduced significantly (see below). This trimmed the 268 million degree 6 polynomials down to 1.6 million. Also, clearly reducible polynomials, such as those with all even exponents or divisible by a

variable, were removed at this point. At each stage data was saved to prevent having to rerun any step.

For speed reasons finding solutions was done by table lookup, so in each orbit the polynomial needing the fewest number of lookups was selected. By choosing the representative with the fewest number of lookups as opposed, for example, to the polynomial with the lowest value of $\alpha(f)$ defined above, 12 million lookups were removed from polynomials of degree 6, resulting in over 3 trillion operations removed during rational point counting.

6.3.3 Timing

After the C program computes all the $\mathbb{F}_q$-rational points, the points are tested for singularities (a singularity will add an additional $\mathbb{F}_q$ rational point only if it comes from resolving a $\mathbb{F}_q$ rational singularity). The computation up to this point took about 80 hours of computer time on a Pentium III 800 MHZ. Using the bounds above on the genus and possible ranges for number of $\mathbb{F}_q$ rational points on the smooth model, the program searched all curves for those with a large number of possible $\mathbb{F}_q$ rational points for each genus and field combination, and all such curves were written out to be examined. If the genus of one of these curves was not forced to be unique using the bounds, the program KANT [27] was used to compute the genus, and this data was incorporated into the C program, and another pass was run. Due to the large number of degree 6 curves, and the length of time to compute the genus of all of them, not all degree 6 curves of genus ≤ 5 were identified. All curves of degree 6, genus ≥ 6 were identified. The C program also found simple points over $\mathbb{F}_2$ to apply the irreducibility theorem above, and then Maple V [34] was used to test for irreducibility since it has multivariable factoring algorithms over finite fields. For 12 curves of degree 6, there were no simple $\mathbb{F}_2$ points, so $\mathbb{F}_4$ simple points were used. For 2 of these curves there were no such simple $\mathbb{F}_4$ points, so $\mathbb{F}_8$ simple points were used. This turned out to suffice to check absolute irreducibility of all polynomials in

this paper. The C program also found the singularity types of the $\mathbb{F}_2$ singularities for visual inspection to see if there were clearly more rational points on the smooth model. The package of [19] was not available to do a more detailed singularity analysis, thus some of the bounds below may be improved by looking for rational points over a wider class of singularities than the $\mathbb{F}_2$ singularities considered here.

The final C code can be found at [32].

6.4 Computational Results

For each field and genus combination polynomials are listed that result in the largest found number of rational points on the smooth model of the curve. For fields $\mathbb{F}_q$, $q = 2^m, m = 3, 4, \ldots, 11$, all homogeneous polynomials in $\mathbb{F}_2[x, y, z]$ of degree ≤ 5 were searched. For $m = 3, 4, \ldots, 9$, the search was extended to include all degree 6 homogeneous polynomials in $\mathbb{F}_2[x, y, z]$. For genus and field combinations not listed here, see [36].

Remark: the four polynomials found in [36] of degree 4, genus 3, with 113 rational points over $\mathbb{F}_{64}$, are only 2 distinct polynomials modulo the action of $GL_3(\mathbb{F}_2)$ on the variables x, y, z.

8 Element Field

A curve of genus 3 and the maximal number of smooth points, 24, is the Klein Quartic

$$x^3\, y + y^3\, z + x\, z^3$$

A genus 5 curve with 28 planar smooth points is

$$x^6 + x^5\, y + x^3\, y^3 + y^6 + y^5\, z + y^4\, z^2 + \left(x^3 + x\, y^2 + y^3\right)\, z^3 + \left(x^2 + x\, y\right)\, z^4 + x\, z^5$$

Note: a reviewer remarked that a genus 5 curve is known with 29 points [51].

A genus 6 curve, with 33 planar smooth points is

$$x^4\,y^2+x^3\,y^3+x\,y^5+x\,y^4\,z+y^4\,z^2+\left(x^2+y^2\right)\,z^4+y\,z^5$$

A curve of genus 7 with 33 smooth planar points is

$$x^6+x^5\,y+x^4\,y^2+x^3\,y^3+y^6+y^5\,z+\left(x^2\,y^2+x\,y^3+y^4\right)\,z^2+\left(x^2\,y+x\,y^2\right)\,z^3+\left(x^2+x\,y+y^2\right)\,z^4$$

A genus 8 curve with 33 smooth planar points is

$$x^5\,y+x^2\,y^4+x\,y^5+y^6+\left(x^4\,y+x^2\,y^3\right)\,z+x^3\,y\,z^2+\left(x^3+x\,y^2\right)\,z^3+x\,y\,z^4+y\,z^5$$

Two curves of genus 9, each with 33 smooth planar points:

$$f_1=x^5\,y+x^4\,y^2+x^2\,y^4+\left(x^3\,y^2+x^2\,y^3\right)\,z+x^4\,z^2+\left(x\,y^2+y^3\right)\,z^3+x^2\,z^4+x\,z^5+z^6$$

$$f_2=x^6+x^4\,y^2+x^3\,y^3+x^2\,y^4+x^3\,y^2\,z+\left(x^4+x^3\,y+x\,y^3\right)\,z^2+y^3\,z^3+(x+y)\,z^5+z^6$$

Five curves of genus 10 with 35 smooth points in the plane:

$$f_1=x^5\,y+x^2\,y^4+y^6+\left(x^3\,y^2+x\,y^4+y^5\right)\,z+y^4\,z^2+\left(x^2\,y+x\,y^2\right)\,z^3+\left(x^2+y^2\right)\,z^4+x\,z^5$$

$$f_2=x^5\,y+x^4\,y^2+x^3\,y^3+x\,y^5+y^6+x^2\,y^3\,z+\left(x^4+x^2\,y^2+x\,y^3\right)\,z^2+x^3\,z^3+y^2\,z^4+x\,z^5+z^6$$

$$f_3=x^5\,y+x^4\,y^2+x^2\,y^4+\left(x^4\,y+y^5\right)\,z+\left(x^4+x\,y^3\right)\,z^2+x^3\,z^3+\left(x^2+y^2\right)\,z^4+y\,z^5+z^6$$

$$f_4=x^5\,y+x^3\,y^3+x^2\,y^4+\left(x^5+x^2\,y^3+y^5\right)\,z+\left(x^2\,y+y^3\right)\,z^3+x^2\,z^4+(x+y)\,z^5+z^6$$

$$f_5=x^4\,y^2+x^2\,y^4+x\,y^5+x^5\,z+x\,y^3\,z^2+\left(x^3+x^2\,y\right)\,z^3+\left(x^2+y^2\right)\,z^4+x\,z^5$$

16 Element Field

One genus 6 curve, a Hermitian curve, with the maximal number of smooth points, 65, was found (it is known to be the unique such curve up to isomorphism):

$$x^5+y^5+z^5$$

Two genus 7 curves each with 57 smooth points in the plane:

$$
\begin{aligned}
f_1 &= x^4 y^2 + x y^5 + y^6 + \left(x^2 y^3 + x y^4 + y^5\right) z + \left(x^2 + x y\right) z^4 + y z^5 \\
f_2 &= x^4 y^2 + x^2 y^4 + y^6 + \left(x^2 y^3 + x y^4\right) z + \left(x^2 + x y\right) z^4 + y z^5
\end{aligned}
$$

A curve with genus 8 with 57 smooth plane points is

$$
x^6 + x^3 y^3 + x^2 y^4 + x^4 y z + x^2 y^2 z^2 + \left(x^3 + x^2 y\right) z^3 + (x + y) z^5
$$

There are two curves of genus 9 with 57 smooth plane points, each receiving two points from blowups: f_1 from the singularity $(1:1:1)$ of type $u^2 + uv + v^2$ which splits over $\mathbb{F}_{16}$, and f_2 from the singularity $(0:1:1)$ of type uv. Thus $N_{16}(9) \geq 59$.

$$
\begin{aligned}
f_1 &= x^5 y + x^3 y^3 + x y^5 + \left(x^5 + y^5\right) z + x^2 y^2 z^2 + \left(x^3 + y^3\right) z^3 + (x + y) z^5 \\
f_2 &= x^6 + x^5 y + x^2 y^4 + y^5 z + x^2 y^2 z^2 + x y^2 z^3 + \left(x^2 + x y\right) z^4 + y z^5
\end{aligned}
$$

The two curves of genus 10 each with 59 plane smooth points are:

$$
f_1 = x^5 y + y^6 + \left(x^2 y^3 + y^5\right) z + \left(x^4 + x^3 y + x y^3\right) z^2 + x y^2 z^3 + (x + y) z^5 + z^6
$$

$$
f_2 = x^5 y + y^6 + \left(x^4 y + x y^4 + y^5\right) z + \left(x^4 + x y^3\right) z^2 + \left(x^3 + x y^2\right) z^3 + y^2 z^4 + z^6
$$

32 Element Field

Three curves with genus 4 and 71 smooth points on the plane curve are:

$$
\begin{aligned}
f_1 &= x^4 y + x y^4 + y^5 + x y^3 z + \left(x y^2 + y^3\right) z^2 + x^2 z^3 + x z^4 + z^5 \\
f_2 &= x^6 + x^3 y^3 + y^6 + \left(x^4 y + y^5\right) z + \left(x^3 y + x^2 y^2\right) z^2 + \left(x^3 + x^2 y + y^3\right) z^3 + \\
&\quad x^2 z^4 + y z^5 + z^6 \\
f_3 &= x^6 + x^3 y^3 + y^6 + \left(x^5 + x^3 y^2 + x^2 y^3\right) z + y^4 z^2 + \left(x^3 + y^3\right) z^3 + y^2 z^4 + x z^5 + z^6
\end{aligned}
$$

A curve with 82 smooth points in the plane and genus 5 is

$$
x^6 + x^3 y^3 + x^2 y^4 + y^6 + x^5 z + x^3 y z^2 + \left(x^3 + x y^2 + y^3\right) z^3 + x^2 z^4 + y z^5
$$

A genus 6 curve with 82 planar smooth points and 2 points above the singularity $(1:0:1)$ of type uv (thus $N_{32}(6) \geq 84$) is

$$x^6 + y^6 + \left(x^4\,y + x^3\,y^2 + x\,y^4\right)\,z + x\,y^2\,z^3 + \left(x^2 + x\,y + y^2\right)\,z^4$$

Two genus 7 curves each with 92 planar smooth points are

$$\begin{aligned} f_1 &= x^3\,y^3 + y^6 + \left(x^5 + x^3\,y^2\right)\,z + \left(x^4 + y^4\right)\,z^2 + \left(x^3 + y^3\right)\,z^3 + y^2\,z^4 + x\,z^5 + z^6 \\ f_2 &= x^6 + y^6 + \left(x^5 + y^5\right)\,z + y^4\,z^2 + \left(x^3 + y^3\right)\,z^3 + x^2\,z^4 + (x+y)\,z^5 \end{aligned}$$

A curve with 93 planar smooth points, genus 8, is

$$x\,y^5 + y^6 + \left(x^5 + x^4\,y\right)\,z + y^4\,z^2 + \left(x^3 + y^3\right)\,z^3 + y^2\,z^4 + y\,z^5$$

A genus 9 curve with 93 smooth planar points:

$$x^4\,y^2 + x^3\,y^3 + \left(x^5 + x^3\,y^2 + x\,y^4 + y^5\right)\,z + x^2\,y^2\,z^2 + \left(x^3 + y^3\right)\,z^3 + x^2\,z^4 + z^6$$

Genus 10 with 103 smooth planar points:

$$x^6 + x^3\,y^3 + x\,y^5 + \left(x^2\,y^2 + x\,y^3\right)\,z^2 + \left(x^3 + x\,y^2 + y^3\right)\,z^3 + x\,y\,z^4 + (x+y)\,z^5$$

64 Element Field

One curve had genus 4 and 118 smooth planar points:

$$x^3\,y^2 + y^5 + y^4\,z + y^2\,z^3 + z^5$$

Two curves of genus 6 had 160 smooth planar points (which is one less than the bound of 161):

$$\begin{aligned} f_1 &= x^4\,y^2 + x^2\,y^4 + x\,y^5 + y^5\,z + y^3\,z^3 + y\,z^5 + z^6 \\ f_2 &= x^6 + x^5\,z + \left(x^4 + y^4\right)\,z^2 + x^3\,z^3 + y^2\,z^4 + y\,z^5 \end{aligned}$$

Genus 7, 153 planar smooth points:

$$x^2\,y^4 + x\,y^5 + y^6 + \left(x^3\,y^2 + x\,y^4 + y^5\right)\,z + x\,y^3\,z^2 + x^2\,z^4 + x\,z^5 + z^6$$

Three curves had genus 8 and 159 plane smooth points, the last two of which have no rational points over $\mathbb{F}_2$:

$$\begin{aligned}
f_1 &= x^3 y^3 + y^6 + \left(x^4 y + x y^4\right) z + \left(x^3 + y^3\right) z^3 + x y z^4 \\
f_2 &= x^6 + x^5 y + x^3 y^3 + x y^5 + y^6 + \left(x^3 y^2 + y^5\right) z + x^3 y z^2 + \left(x^2 y + y^3\right) z^3 + \\
&\quad y^2 z^4 + x z^5 + z^6 \\
f_3 &= x^6 + x^4 y^2 + x^3 y^3 + x^2 y^4 + y^6 + \left(x^4 + x^2 y^2 + y^4\right) z^2 + \left(x^3 + y^3\right) z^3 + \\
&\quad \left(x^2 + y^2\right) z^4 + z^6
\end{aligned}$$

There are 166 plane smooth points on this curve of genus 9:

$$x^6 + x^3 y^3 + \left(x^4 y + x^2 y^3\right) z + \left(x^3 y + x y^3 + y^4\right) z^2 + x^2 z^4 + y z^5$$

Four genus 10 curves each had 171 points on their smooth model:

$$\begin{aligned}
f_1 &= x^6 + y^6 + \left(x^4 y + x^2 y^3 + x y^4\right) z + x^3 y z^2 + x y^2 z^3 + x y z^4 + z^6 \\
f_2 &= x^6 + x^5 y + x^4 y^2 + x^3 y^3 + x^2 y^4 + x y^5 + y^6 + \left(x^4 y + x y^4\right) z + \left(x^2 y + x y^2\right) z^3 + z^6 \\
f_3 &= x^6 + x^3 y^3 + y^6 + \left(x^4 y + x y^4\right) z + \left(x^3 + y^3\right) z^3 + z^6 \\
f_4 &= x^6 + x^3 y^3 + x y^5 + x^3 y^2 z + \left(x^4 + x^3 y + y^4\right) z^2 + y^2 z^4 + x z^5 + z^6
\end{aligned}$$

128 Element Field

There is one degree 6 plane curve with a genus 3 smooth model, with 183 smooth plane points, and another point coming from the singularity $(0:0:1)$ of type $(u+v)(u^2+uv+v^2)$, which matches [36]. The curve is

$$x^6 + x^5 y + x^4 y^2 + x^3 y^3 + x^2 y^4 + \left(x^5 + x^4 y\right) z + y^4 z^2 + \left(x^3 + y^3\right) z^3$$

A curve of genus 4 with 215 planar smooth points (2 less than the maximum possible) is

$$x^2 y^3 + x y^4 + x^4 z + x y^2 z^2 + x y z^3 + (x + y) z^4$$

There are two curves of genus 6 with 240 planar smooth points, receiving 3 points each from singularities. f_1 has type $uv(u+v)$ at $(0:1:0)$ and f_2 has type $(u+v)(u^2+uv+v^2)$ at $(0:1:0)$ and type uv at $(1:0:0)$. Thus $N_{128}(6) \geq 243$.

$$\begin{aligned} f_1 &= x^4\,y^2 + \left(x^5 + x^4\,y + x^2\,y^3\right)\,z + \left(x^2\,y^2 + x\,y^3\right)\,z^2 + \left(x^2 + x\,y + y^2\right)\,z^4 \\ f_2 &= x^3\,y^3 + x^4\,y\,z + \left(x^4 + x^3\,y\right)\,z^2 + \left(x^3 + x^2\,y + y^3\right)\,z^3 + z^6 \end{aligned}$$

Two genus 7 curves with 248 smooth planar points:

$$\begin{aligned} f_1 &= x^3\,y^3 + x\,y^5 + y^6 + x^3\,y^2\,z + y^4\,z^2 + x^3\,z^3 + \left(x^2 + y^2\right)\,z^4 + (x+y)\,z^5 \\ f_2 &= x^5\,y + x^4\,y^2 + x^2\,y^4 + \left(x^3\,y^2 + x^2\,y^3\right)\,z + x^4\,z^2 + x\,y^2\,z^3 + z^6 \end{aligned}$$

A curve with 266 planar smooth points, genus 8, and no $\mathbb{F}_2$ rational points is

$$x^6 + x^3\,y^3 + x^2\,y^4 + x\,y^5 + y^6 + \left(x^5 + y^5\right)\,z + \left(x^2\,y^2 + y^4\right)\,z^2 + \left(x^3 + y^3\right)\,z^3 + x\,z^5 + z^6$$

There are 269 smooth plane points on the curves of genus 9 given by

$$\begin{aligned} f_1 &= x^4\,y^2 + x\,y^5 + \left(x^4 + y^4\right)\,z^2 + \left(x^3 + y^3\right)\,z^3 + x\,y\,z^4 + x\,z^5 + z^6 \\ f_2 &= x^6 + x^3\,y^3 + x^2\,y^4 + y^6 + \left(x\,y^4 + y^5\right)\,z + x^2\,y^2\,z^2 + \left(x^2 + x\,y + y^2\right)\,z^4 \end{aligned}$$

The smooth curve of genus 10 with 276 $\mathbb{F}_{128}$ rational points is

$$x^6 + y^6 + x^2\,y^3\,z + \left(x^4 + x^3\,y + y^4\right)\,z^2 + x^3\,z^3 + x^2\,z^4 + x\,z^5$$

256 Element Field

A genus 3 curve not listed in [36] with 350 smooth planar points is given by

$$x^5 + x\,y^4 + y^5 + \left(x^2\,y^2 + y^4\right)\,z + \left(x^2\,y + x\,y^2\right)\,z^2 + x\,z^4 + z^5$$

A curve with 399 smooth plane points and genus 5 is

$$x^6 + x^4\,y^2 + x^5\,z + \left(x^2\,y^2 + y^4\right)\,z^2 + \left(x^2\,y + x\,y^2\right)\,z^3 + x^2\,z^4 + y\,z^5$$

A genus 6 curve with 416 smooth plane points is

$$x^4\,y + x^3\,y^2 + y^4\,z + \left(x^3 + y^3\right)\,z^2 + \left(x^2 + x\,y\right)\,z^3 + z^5$$

One point from the singularity $(1:0:0)$ of type uv^2 is added to the 442 smooth plane points on a curve of genus 7 given by

$$x^3\,y^3 + x^2\,y^4 + y^5\,z + x^3\,y\,z^2 + \left(x\,y^2 + y^3\right)\,z^3 + y^2\,z^4 + z^6$$

A curve of genus 8 with one point less than the Serre bound has 512 smooth plane points and is given by

$$x^4\,y^2 + y^5\,z + x\,z^5$$

Two curves of genus 9, each with 474 smooth points and 2 points from singularities of type $u^2 + uv + v^2$, which factor over $\mathbb{F}_{256}$, at points $(0:1:1)$ and $(1:1:0)$ respectively (so $N_{256}(9) \geq 476$) are

$$\begin{aligned} f_1 &= x^5\,y + x^3\,y^3 + x^2\,y^4 + x\,y^5 + y^4\,z^2 + x^3\,z^3 + y^2\,z^4 + x\,z^5 \\ f_2 &= x^6 + y^6 + \left(x^5 + y^5\right)\,z + x^4\,z^2 + \left(x^2\,y + x\,y^2\right)\,z^3 + x\,z^5 + z^6 \end{aligned}$$

Two smooth curves of genus 10 have 537 smooth plane points:

$$\begin{aligned} f_1 &= x^6 + x\,y^5 + x^4\,y\,z + x^2\,y^2\,z^2 + y^3\,z^3 + x\,z^5 \\ f_2 &= x^6 + x^5\,y + x^3\,y^3 + x\,y^5 + y^6 + \left(x^5 + y^5\right)\,z + x^2\,y^2\,z^2 + x\,y\,z^4 + z^6 \end{aligned}$$

512 Element Field

Four curves overlooked in [36] of genus 4 have 663 plane smooth points. They are

$$\begin{aligned} f_1 &= x^4\,y + x\,y^4 + \left(x^3\,y + y^4\right)\,z + \left(x\,y + y^2\right)\,z^3 + z^5 \\ f_2 &= x^4\,y + x\,y^4 + y^5 + \left(x\,y^3 + y^4\right)\,z + \left(x\,y^2 + y^3\right)\,z^2 + x^2\,z^3 + x\,z^4 \\ f_3 &= x^4\,y + x^2\,y^3 + y^5 + \left(x^2\,y^2 + x\,y^3 + y^4\right)\,z + \left(x^3 + y^3\right)\,z^2 + z^5 \\ f_4 &= x^5 + y^5 + \left(x^4 + x^3\,y + y^4\right)\,z + \left(x\,y^2 + y^3\right)\,z^2 + z^5 \end{aligned}$$

A genus 6 curve with 766 smooth plane points and one more point from the singularity $(1:0:0)$ of type $(u+v)(u^2+uv+v^2)$ (so $N_{512}(6) \geq 767$) is

$$x^3\,y^3 + y^6 + \left(x\,y^4 + y^5\right)\,z + \left(x^2\,y^2 + y^4\right)\,z^2 + x^3\,z^3 + x\,y\,z^4 + (x+y)\,z^5$$

There are 786 smooth plane points and 1 point from the singularity $(1:0:0)$ of type uv^2 on the genus 7 curve

$$x^2\,y^4 + y^6 + x^3\,y^2\,z + \left(x^3 + x\,y^2\right)\,z^3 + x\,y\,z^4 + y\,z^5$$

A curve of genus 8 with 813 plane smooth points is

$$x^2\,y^4 + y^6 + \left(x^5 + x^2\,y^3\right)\,z + \left(x^3\,y + x\,y^3 + y^4\right)\,z^2 + \left(x^3 + x^2\,y\right)\,z^3 + x\,z^5$$

A genus 9 curve with 837 smooth plane points is

$$x^6 + x^4\,y^2 + \left(x\,y^4 + y^5\right)\,z + x^2\,y^2\,z^2 + \left(x^2\,y + x\,y^2\right)\,z^3 + x\,y\,z^4 + x\,z^5 + z^6$$

A smooth genus 10 plane curve with 845 plane points is

$$x^5\,y + x^4\,y^2 + x^2\,y^4 + y^6 + \left(x^2\,y^3 + y^5\right)\,z + \left(x^3\,y + y^4\right)\,z^2 + x^2\,z^4 + (x+y)\,z^5$$

1024 Element Field

A genus 3 curve with 1211 smooth plane points is

$$x^3\,y + y^3\,z + y\,z^3 + z^4$$

Three genus 4 curves have 1273 smooth plane points:

$$\begin{aligned} f_1 &= x^3\,y^2 + y^5 + x^2\,y\,z^2 + y^2\,z^3 + x\,z^4 \\ f_2 &= x^4\,y + x^2\,y^3 + y^5 + \left(x^2\,y^2 + y^4\right)\,z + \left(x^3 + y^3\right)\,z^2 + x\,z^4 \\ f_3 &= x^5 + x^3\,y^2 + x^2\,y^3 + y^5 + y^4\,z + x\,y^2\,z^2 + x^2\,z^3 \end{aligned}$$

A curve with 1343 smooth plane points, genus 5, and 2 points coming from the singularity $(1:0:0)$ of type uv (and thus attaining the maximum possible 1345) is

$$x^3\,y^2 + y^5 + x^3\,y\,z + y^3\,z^2 + z^5$$

A genus 6 curve with 1383 smooth plane points is

$$x^4\,y + x\,y^4 + y^5 + x^2\,y^2\,z + x\,y\,z^3 + z^5$$

2048 Element Field

Two genus 3 curves with 2293 smooth plane points, and one more coming from the singularity $(0:1:0)$ of type $(u+v)(u^2+uv+v^2)$ on each curve are

$$f_1 = x^4\,y + x^3\,y^2 + x^3\,y\,z + y^2\,z^3 + (x+y)\;z^4$$

$$f_2 = x^4\,y + x^3\,y^2 + x^3\,y\,z + x^3\,z^2 + y^2\,z^3 + y\,z^4$$

Three curves with 2380 smooth plane points and genus 4 are

$$\begin{aligned} f_1 &= x^5 + y^5 + x^3\,y\,z + y^2\,z^3 + x\,z^4 \\ f_2 &= x^5 + x^4\,y + \left(x\,y^3 + y^4\right)\;z + x^3\,z^2 + \left(x^2 + y^2\right)\;z^3 + z^5 \\ f_3 &= x^5 + x^2\,y^3 + x\,y^4 + x^4\,z + x^3\,z^2 + \left(x^2 + x\,y + y^2\right)\;z^3 + x\,z^4 + z^5 \end{aligned}$$

A genus 5 curve with 2422 smooth plane points is

$$x^4\,y + x^3\,y^2 + y^5 + x\,y^2\,z^2 + \left(x^2 + x\,y + y^2\right)\;z^3$$

Finally, a genus 6 curve with 2556 planar smooth points is

$$x^4\,y + x^2\,y^3 + x\,y^4 + y^5 + \left(x^3\,y + y^4\right)\;z + x^2\,z^3 + y\,z^4$$

6.5 Tallies

The columns headed “bound” give the Serre [46] bound, unless marked [26] as Ihara or [29] as Lauter. The columns headed “best” give the lower bounds for $N_q(g)$ found above; bounds marked [36] and [46] are from those previous papers. Note in particular the reduction from the Serre [46] upper bounds using [26] and [29] has made several known curves closer to or already optimal. After this paper was initially written in 2000, improved bounds were published in [25] and incorporated in this table. These new bounds made the $q = 128$, $g = 4$ curve optimal.

Table 6.1
Known Bounds on Number of Rational Points on Curves

F_q	best 3	bound 3	best 4	bound 4	best 5	bound 5	best 6	bound 6
8	24 [46]	24	25 [36]	25 [25]	28	30 [25]	33	35 [29]
16	38 [46]	41	45 [36]	45 [25]	45 [36]	53 [25]	65	65
32	63 [36]	65 [29]	71	74 [25]	82	85 [25]	84	96 [25]
64	113 [36]	113	118	129	130 [36]	145	160	161
128	184 [36]	195	215	215 [25]	227 [36]	239	243	258 [25]
256	350 [36]	353	381 [36]	385	399	417	416	449
512	640 [36]	648	663	693	724 [36]	738	767	783
1024	1211	1217	1273	1281	1345	1345	1383	1409
2048	2294	2319	2380	2409	2422	2499	2556	2589
F_q	best 7	bound 7	best 8	bound 8	best 9	bound 9	best 10	bound 10
8	33	38 [25]	33	42 [25]	33	45 [25]	35	49 [25]
16	57	69 [25]	57	75 [25]	59	81 [26]	59	87 [26]
32	92	107 [25]	93	118 [25]	93	128 [25]	103	139 [25]
64	153	177	159	193	166	209	171	225
128	248	283	266	302 [25]	269	322 [25]	276	349
256	443	481	512	513	476	545	537	577
512	787	828	813	873	837	918	845	963

6.6 Comments

The techniques used here make a search over degree 7 plane curves feasible on a supercomputer, and quite possibly on a home PC. The desingularized curves can be used to construct algebraic-geometric Goppa codes [40], [49]. For example, using the genus 5 curve over $\mathbb{F}_{1024}$ with 1345 rational points, linear codes with parameters $[n, k-4, n-k]$ can be constructed for $10 \leq n \leq 1344$ and $8 < k < n$ over $\mathbb{F}_{1024}$. Similarly, using the genus 6 $\mathbb{F}_{64}$ curve with 160 points, $[n, k-5, n-k]$-linear codes can be constructed for $12 \leq n \leq 159$ and $10 < k < n$, and the $\mathbb{F}_{256}$ curve of genus 8 with 512 rational points gives $[n, k-7, n-k]$-linear codes for $16 \leq n \leq 511$ and $14 < k < n$ (see, for example, [40]).

Thanks to the reviewer for numerous suggestions on layout and a few corrections.

For conclusions and open problems see section 7.4.

7. CONCLUSION AND OPEN PROBLEMS

7.1 Codes Obtained

Codes resulting from ruled surfaces over $\mathbb{P}^1$ are completely classified in this thesis. Although these Lomont codes #1 still suffer from having a fixed length like the Reed Solomon codes, the Lomont codes #1 are usable in some situations where the product Reed Solomon fails. For example, the Lomont codes #1 can correct longer burst errors over the same fixed field, perhaps making hardware implementations more cost efficient. Decoding them using the methods for a (product) of Goppa codes is still not as efficient as decoding Reed Solomon codes, so there is still work to do on decoding.

For the codes resulting from ruled surfaces over elliptic curves, the degree 1 bundle case is left open, and is tantalizingly close to being solvable. To do this one needs some classification of symmetric powers similar to theorem 5.4.1, but for the rank 2 indecomposable bundle of degree 1. The codes from degree 0 bundles are comparable to the product code of a Reed Solomon and and a Goppa code, but perhaps a more efficient decoding algorithm could be found for the Lomont code #2 than the product code, making it also useful in practice.

Open Problem 7.1.1 (Decoding Lomont Codes) *Find an efficient algorithm to decode the codes from theorems 5.2.1 and 5.4.3. A good start is looking at current Goppa code decoding algorithms, say from Pretzel's book [40].*

Open Problem 7.1.2 (Genus 2 classification) *Similar to the codes in theorems 5.2.1 and 5.4.3, classify codes resulting from surfaces ruled over curves of genus 2.*

Curves of Garcia-Stichtenoth

Since good families of codes require long codes, and the curves explicitly described in this section give Goppa codes reaching the Drinfeld-Vladut bound, it might be useful to study ruled surfaces over these curves. In particular, since equations are given below for the family of curves, and the number of rational points and genus is known for each curve, computer algorithms could be developed to study properties of the resulting surface codes.

In 1995, A. Garcia and H. Stichtenoth gave explicit construction of these two families of curves (GS curves) meeting the TVZ bound (theorem 2.4.3) [13], [14]. In the language of function fields, the G-S curves form towers $F_1, F_2, F_3, \ldots, F_n, \ldots$ of Artin-Schreier extensions of the rational function field $\mathbb{F}_{q^2}(x_1)$. The first family is given by

$$\begin{aligned} F_1 &= \mathbb{F}_{q^2}(x_1) \\ F_{n+1} &= F_n(x_{n+1}), \quad n \geq 1 \\ x_{n+1}^q + x_{n+1} &= \frac{x_n^q}{x_n^{q-1}+1}, \quad n \geq 0 \end{aligned}$$

For the first family, the genus $g(F_n)$ of F_n is shown to be

$$g(F_n) = \begin{cases} (q^{i+1}-1)(q^{i-1}-1), & : \quad n = 2i+1 \text{ odd} \\ (q^i-1)^2, & : \quad n = 2i \text{ even} \end{cases}$$

and the smooth curve corresponding to the function field F_n has at least $(q-1)q^n$ $\mathbb{F}_q$ rational points. Thus $\limsup_{n\to\infty} N_n/g_n(F_n) = q-1$, the Drinfeld-Vladut bound [10].

The second family is given by

$$\begin{aligned} F_1 &= \mathbb{F}_{q^2}(x_1) \\ F_{n+1} &= F_n(z_{n+1}), \quad n \geq 1 \\ z_{n+1}^q + z_{n+1} &= x_n^{q+1} \\ x_n x_{n-1} &= z_n \quad n \geq 2 \end{aligned}$$

The genus and number of points is known for the second family as well, and it too reaches the Drinfeld-Vladut bound.

It would be worthwhile to study general rank 2 vector bundles over these curves, in order to construct the corresponding surfaces and then codes. For decomposable vector bundles, the answers were given above in section 5.3, and are product codes, so cannot beat the best current codes. But for more general vector bundles programs could be written to investigate the parameters, perhaps resulting in some good surface codes.

7.2 Other Surface Types

There are codes obtainable from any other surface types, and perhaps by applying theorem 3.2.5 some code parameters could be deduced. Some study of the classification of surfaces would be needed.

7.3 Higher Dimensional Varieties

The theory of higher dimensional varieties is not as well developed as that for curves and surfaces, but there would be codes here too, although I expect the problem of determining the code parameters much more difficult than in the curve or surface case. From a suggestion of Kenji Matsuki, it seems that studying codes using the code definition 2.5.1 applied to $\mathbb{P}^n$ may be solvable.

Open Problem 7.3.1 ($\mathbb{P}^n$ codes) *From the definition 2.5.1 applied to $\mathbb{P}^n$, find code parameters and a decoding algorithm.*

7.4 New Projective Curves

The search in chapter 6 for explicit curves meeting known bounds on number of rational points also has several possible extensions. Previously known results are [36] and [46]. The bounds in this paper could possibly be strengthened by by analyzing the singularities in more detail, resulting in more known $\mathbb{F}_q$ rational points on the smooth models of the curves. Also all genus ≤ 5 curves from the degree 6 polynomials

were not identified. More work could be done to compute exact parameters for these curves.

Since computing power grows quickly, the range of curves searched should be easily done by the time this is in print. For example:

Open Problem 7.4.1 (Find more curves) *Extend the techniques of chapter 6 on new curves to search larger spaces, like all degree 7 curves or extend the coefficient field to $\mathbb{F}_4$ or larger.*

LIST OF REFERENCES

[1] J. d'Almeida, A. Hirschowitz, *Quelques plongements non-spéciaux de surfaces rationelles*, Math. Z. **211**, pp. 479-483, (1992).

[2] J.K. Arason, R. Elman, and B. Jacob, *On indecomposable vector bundles*, Comm. Algebra **20**, no. 5, pp. 1323-1351, (1992).

[3] M.F. Atiyah, *Vector bundles over an elliptic curve*, Proc. London Math. Soc., **7**, pp. 414-452, (1957).

[4] Edoardo Ballico and Marc Coppens, *Very ample line bundles on blown-up projective varieties*, Bull. Belg. Math Soc. **4**, pp. 437-447, (1997).

[5] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, *Quantum Error Correction Via Codes Over GF(4)*, IEEE Trans. Information Theory, 44 (1998), pp. 1369-1387; http://xxx.lanl.gov/quant-ph/9608006.

[6] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *Quantum error correction and orthogonal geometry*, Phys. Rev. Lett. **78**, pp. 405-408, 1997; http://xxx.lanl.gov/abs/quant-ph/9605005.

[7] Marc Coppens, *Embeddings of general blowing-ups at points*, J. Reine Agnew. Math., **469** pp. 179-198, (1995).

[8] Marc Coppens, *Very ample linear systems on blowings-up at general points of projective spaces*, Canad. Math. Bull., **45**(3), pp. 349-354, (2002).

[9] Marc Coppens, *Very ample linear systems on blowings-up at general points of smooth projective varieties*, Pacific Journal of Mathematics,

202, No 2, pp. 313-327, (2002).

[10] V. G. Drinfeld and S. G. Vlăduţ, *Number of points of an algebraic curve*, Func. Anal. And Appl., **17**, pp. 53-54, (1983).

[11] D. Eisenbud, *Commutative Algebra with a view towards Algebraic Geometry*, GTM#150, Springer-Verlag, (1995).

[12] W. Fulton, *Intersection Theory*, Second Edition, Springer, (1998).

[13] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vlăduţ bound*, Invent. Math., vol 121, pp. 211-222, 1995.

[14] A. Garcia and H. Stichtenoth, *Asymptotically good towers of function fields over finite fields*, C. R. Acar. Sci. Paris Sér. I Math., **322**, pp. 1067-1070, (1996).

[15] M. J. E. Golay *Notes on digital coding*, Proc. I.R.E, **37**, p. 657, (1949).

[16] V.D. Goppa, *Codes on algebraic curves*, Sov. Math.-Dokl., Vol. 24, pp. 170-172, (1981).

[17] R. Graham, D. Knuth, O. Patashnik, *Concrete Mathematics, A Foundation for Computer Science*, Addison-Wesley, (1989, 1994).

[18] A. Grothendieck, *Sur la classification des fibres holomorphes sur la sphére de Riemann*, Amer. J. Math. **79**, pp. 121-38, (1957).

[19] G. Haché and D. Le Brigand, *Effective construction of algebraic-geometric codes*, IEEE Transactions on Information Theory, vol. 41, pp. 1615-1628, (Nov 1995).

[20] R. W. Hamming, *Error detecting and error correcting codes*, Bell Syst. Tech. J., **26**, 2, April 1950.

[21] S. H. Hanson, *The geometry of Deligne-Lusztig varieties; Higher dimensional AG codes*, Ph. D. Thesis, University of Aarhus, Department of Mathematical Sciences, University of Aarhus, DK-800 Aarhus C, Denmark, July 1999.

[22] R. Hartshorne, *Algebraic Geometry*, GTM#52, Springer-Verlag, (1977).

[23] R. Hartshorne, *Resides and duality; lecture notes on the work of A. Grothendieck, given at Harvard 63/64*, Berlin-New York, Springer-Verlag, (1966).

[24] R. Hartshorne, *Ample bundles on curves*, Nagoya Math. J., **43**, pp. 73-89, (1971).

[25] E. Howe, K. Lauter, http://arxiv.org/abs/math.NT/0207101

[26] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokyo, 28, pp. 721-724, (1981).

[27] KANT, http://www.math.tu-berlin.de/algebra

[28] Oliver Küchle, *Ample line bundles on blown up surfaces*, http://xxx.lanl.gov/abs/alg-geom/9410011

[29] K. Lauter, *Geometric methods for improving the upper bounds of the number of rational points on algebraic curves over finite fields*, Journal of Algebraic Geometry, 10, pp. 19-36, (2001).

[30] J.H. van Lint, *Introduction to Coding Theory*, GTM#86, Springer-Verlag, (1982).

[31] C. Lomont, *Yet more projective curves over* $\mathbb{F}_2$, to appear in Exp. Math.

[32] www.math.purdue.edu/∼clomont/Math/Papers/2000/PolySolver.zip

[33] D. A. Mac Dónaill, *A parity code interpretation of nucleotide alphabet composition*, Chemical Communications, pp. 2062 - 2063, (2002).

[34] MAPLE, www.maplesoft.com

[35] C. Moreno, *Algebraic Curves over Finite Fields*, Cambridge Tracts in Mathematics, Cambridge University Press, (1991).

[36] O. Moreno, D. Zinoviev, V. Zinoviev, *On several new projective curves over* F_2 *of Genus 3, 4, and 5*, IEEE Transactions on Information Theory, vol. 41, pp. 1643-1648, (Nov 1995).

[37] J. B. Hans Peek, *Communications aspects of the compact disc audio system*, IEEE Communications Magazine, Vol 23, No 2, pp. 7-15 (Feb 1985).

[38] Bjorn Poonen, *Bertini theorems over finite fields*, preprint.

[39] E. C. Posner, *Combinatorial structures in planetary reconaissance*, in Error Correcting Codes, edited by H. B. Mann, pp. 15-46, New York-London-Sydney-Toronto: Wiley (1968).

[40] O. Pretzel, *Codes and Algebraic Curves*, Oxford Science Publications, Clarendon Press, (1998).

[41] J. Ragot, http://pauillac.inria.fr/algo/seminars/sem97-98/ragot.html

[42] I. S. Reed and G. Solomon, *Polynomial codes over certain finite fields*, SIAM J. Appl. Math., Vol 8, No 2, pp. 300-304 (June 1960).

[43] S. Roman, *Coding Theory and Information Theory*, GTM#134, Springer-Verlag, (1992).

[44] R. L. E. Schwarzenberger, *Vector bundles on the projective plane*, Proc. London Math. Soc., (3) 11, pp. 623-40, (1961).

[45] J.-P. Serre, *Faisceaux algébriques cohérents*, Ann. of Math., **61**, pp. 1-42 (1955).

[46] J.-P. Serre, *Nombres de points des courbes algebriques sur* F_q, Seminaire de Theorie des Nombres de Bordeux, expose 22, pp. 1-8, (1983).

[47] C.E. Shannon, *A mathematical theory of commumication*, Bell Syst. Tech. J., **27**, pp. 379-423, 623-656, (1948).

[48] P. W. Shor, *Fault-tolerant quantum computation*, Proc. 35th Ann. Symp. on Fundamentals of Computer Science(IEEE Press, Los Alamitos, 1996), pp. 56-65; http://xxx.lanl.giv/abs/quant-ph/9605011.

[49] M. A. Tsfafman and S. G. Vlăduţ, *Algebraic-Geometric Codes*. Dordrecht/Boston/London: Kluwer, (1991).

[50] M.A. Tsfasman, S.G. Vlăduţ, and Th. Zink, *On Goppa codes which are better than the Varshamov-Gilbert bound*, Math Nachr, **109**, pp. 21-28, (1982).

[51] van der Geer/van der Vlugt tables at http://www.science.uva.nl/∼geer/

[52] R. Walker, *Algebraic Curves*, Dover Publications, N.Y., 1962.

[53] http://www.spectrum.ieee.org/WEBONLY/pressrelease/0701/0701dig.pdf

[54] Geng Xu, *Ample line bundles on smooth surfaces*, J. Reine Agnew. Math., **469**, pp. 199-209, (1995).

(This page deliberately left blank.)

APPENDIX - SHEAF RESULTS

Here are collected a few results needed in this thesis that probably appear in the literature, but I was unable to find them.

We use the following definition of the binomial coefficient:

Definition A.1.2 *Binomial Coefficient [17, 5.1]*

$$\binom{r}{k} = \begin{cases} \frac{r(r-1)(r-2)\dots(r-k+1)}{k!} & k \geq 0 \\ 0 & k < 0 \end{cases}$$

for $r \in \mathbb{R}$ and k an integer.

Then,

Lemma A.1.3

$$\sum_{j=0}^{n} \binom{j+m}{m} = \binom{m+n+1}{m+1}$$

Proof $\sum_{j=0}^{n} \binom{j}{m} = \binom{n+1}{m+1}$, called "*upper summation*" from [17, 5.10].

Then

$$\begin{aligned} \sum_{j=0}^{n} \binom{j+m}{m} &= \sum_{k=m}^{m+n} \binom{k}{m} \\ &= \sum_{k=0}^{m+n} \binom{k}{m} - \sum_{k=0}^{m-1} \binom{k}{m} \\ &= \binom{m+n+1}{m+1} - \binom{m}{m+1} \\ &= \binom{m+n+1}{m+1} \end{aligned}$$

where the last term in the second to last line is 0 by definition.

∎

Theorem A.1.4 *For vector bundles $\mathcal{E}$ and $\mathcal{F}$ over a curve C*

$$\deg(\mathcal{E} \otimes \mathcal{F}) = \mathit{rank}\, \mathcal{F} \deg \mathcal{E} + \mathit{rank}\, \mathcal{E} \deg \mathcal{F}$$

Proof Let $\mathcal{E}$ have rank r, and $\mathcal{F}$ have rank s. Then by [22, Appendix A, C4] the Chern polynomials are

$$c_t(\mathcal{E}) = \prod_{i=1}^{r}(1 + a_i t)$$

and

$$c_t(\mathcal{F}) = \prod_{j=1}^{s}(1 + b_j t),$$

where the a_i and b_j are formal symbols. From [22, Appendix A, C5] or [12, Remark 3.2.3 (b),(c)] we then use

$$c_t(\mathcal{E} \otimes \mathcal{F}) = \prod_{i,j}(1 + (a_i + b_j)t)$$

and the Chern polynomial of an exterior power gives

$$\begin{aligned} c_t(\wedge^{r+s}(\mathcal{E} \otimes \mathcal{F})) &= 1 + t\sum_{i,j}(a_i + b_j) \\ &= 1 + t(s\sum_i a_i + r\sum_j b_j) \end{aligned}$$

Since the degree of the sheaf in the Riemann-Roch theorem [22, Appendix A, Example 4.1.1] comes solely from the $s\sum a_i + r\sum b_j$ term, and since $c_t(\wedge^r \mathcal{E}) = 1 + t\sum a_i$, etc., we get the result. ∎

Next we compute the rank and degree of $S^n(\mathcal{E})$ where $\mathcal{E}$ is a vector bundle of rank r and degree d over a curve C.

Theorem A.1.5 ***If*** *$\mathcal{E}$ is a rank r degree d vector bundle over a curve C,* ***then***

$$\textit{rank } S^n(\mathcal{E}) = \binom{n + r - 1}{r - 1}$$

Proof Since rank is local, and $\mathcal{E}$ is locally free, let R be a local ring, and compute rank $S^n(M)$, where $M = \bigoplus_{i=0}^{r} R$. $S(M) \cong R[x_1, x_2, \ldots, x_r]$ [11, Cor A2.3c]. Then rank $S^n(M) = \{\#\text{ of monomials of degree } n\} = \binom{n+r-1}{r-1}$. ∎

The degree is harder to compute. If rank $\mathcal{E} = 1$, then $\mathcal{E}$ is a line bundle, and $\deg S^n(\mathcal{E}) = n \deg \mathcal{E}$. So assume rank $\mathcal{E} \geq 2$. First, applying the splitting principle [12, Remark 3.2.3] to $\mathcal{E}$,

$$\mathcal{E} = \mathcal{E}_r \supseteq \mathcal{E}_{r-1} \supseteq \cdots \supseteq \mathcal{E}_1 \supseteq \mathcal{E}_0 = 0$$

with rank $\mathcal{E}_i = i$, line bundles $\mathcal{L}_i = \mathcal{E}_i/\mathcal{E}_{i-1}$, for $i = 1, 2, \ldots, r$. Then applying [22, II, exercise 5.16(c)] to $0 \to \mathcal{E}_{r-1} \to \mathcal{E} \to \mathcal{L}_r \to 0$, we have the filtration

$$S^n(\mathcal{E}) = F^0 \supseteq F^1 \supseteq \cdots \supseteq F^n \supseteq F^{n+1} = 0$$

and sequences

$$\begin{array}{ccccccccccc}
0 & \to & F^1 & \to & S^n(\mathcal{E}) & \to & S^0(\mathcal{E}_{r-1}) & \otimes & S^n(\mathcal{L}_r) & \to & 0 \\
0 & \to & F^2 & \to & F^1 & \to & S^1(\mathcal{E}_{r-1}) & \otimes & S^{n-1}(\mathcal{L}_r) & \to & 0 \\
 & & & & & \vdots & & & & & \\
0 & \to & F^n & \to & F^{n-1} & \to & S^{n-1}(\mathcal{E}_{r-1}) & \otimes & S^1(\mathcal{L}_r) & \to & 0 \\
0 & \to & F^{n+1} & \to & F^n & \to & S^n(\mathcal{E}_{r-1}) & \otimes & S^0(\mathcal{L}_r) & \to & 0
\end{array}$$

From [22, II, exercise 5.16 (d)] degree is additive across exact sequences, so we get that

$$\deg S^n(\mathcal{E}) = \sum_{k=0}^{n} \deg(S^k(\mathcal{E}_{r-1}) \otimes S^{n-k}(\mathcal{L}_r)) \tag{A.1}$$

Hartshorne states [24, proving prop. 2.3] without proof the following theorem (and it was not clear in his proof what restrictions were on the bundles other than being over a curve):

Theorem A.1.6 *Let $\mathcal{E}$ be a vector bundle over a curve, of rank r and degree d.* ***Then***

$$\deg S^n(\mathcal{E}) = \frac{dn}{r}\binom{n+r-1}{r-1}$$

Note A.1.7 Kenji Matsuki noted that this proof can be done in the much simpler case $\mathcal{E} = \oplus \mathcal{L}_i$, a sum of line bundles, by using the splitting principle. I will leave the sequences above, since they may provide tools in some cases to compute the dimension $k = h^0(C, S^a(\mathcal{E}) \otimes \mathcal{O}_C(bP_0))$ for general vector bundles over curves, as needed in theorem 5.1.4.

Proof We induct using the above formulas. For rank 1 it is true from equation A.1 above. Assume $\deg \mathcal{E}_{r-1} = d_1$ and $\deg \mathcal{L}_r = d_2$, giving $d = d_1 + d_2$. Then

$$\begin{aligned}
\deg S^n(\mathcal{E}) &= \sum_{k=0}^{n} \deg(S^k(\mathcal{E}_{r-1}) \otimes S^{n-k}(\mathcal{L}_r)) \\
&= \sum \tbinom{k+r-2}{r-2}(n-k)d_2 + \tfrac{kd_1}{r-1}\tbinom{k+r-2}{r-2} \\
&= \sum(-d_2 + \tfrac{d_1}{r-1})(\tfrac{k+r-1}{r-1})(r-1)\tbinom{k+r-2}{r-2} + [nd_2 - (r-1)(-d_2 + \tfrac{d_1}{r-1})]\tbinom{k+r-2}{r-2} \\
&= \sum(d_1 - (r-1)d_2)\tbinom{k+r-1}{r-1} + \sum[nd_2 - (d_1 - (r-1)d_2)]\tbinom{k+r-2}{r-2}
\end{aligned}$$

where to get to the last line we used the identity $\frac{k+r-1}{r-1}\binom{k+r-2}{r-2} = \binom{k+r-1}{r-1}$, $r \neq 1$ [17, 5.5]. Applying lemma A.1.3 twice the sum becomes

$$\begin{aligned}
&= [d_1 - (r-1)d_2]\tbinom{n+r}{r} + [nd_2 - (d_1 - (r-1)d_2)]\tbinom{n+r-1}{r-1} \\
&= [\tfrac{n+r}{r}(d_1 - (r-1)d_2) + nd_2 - d_1 + (r-1)d_2]\tbinom{n+r-1}{r-1} \\
&= [\tfrac{nd_1}{r} + \tfrac{nd_2}{r}]\tbinom{n+r-1}{r-1} \\
&= \tfrac{nd}{r}\tbinom{n+r-1}{r-1}
\end{aligned}$$

Where we again used [17, 5.5] in the form $\binom{n+r}{r} = \frac{n+r}{r}\binom{n+r-1}{r-1}$. This completes the proof. ■

VITA

"A little nonsense now and then is relished by the wisest men" - Willy Wonka

Chris Lomont was born December 12, 1968, in Fort Wayne, Indiana, where he spent his youth "experimenting", which consisted of explosions and fire. 18 years later, after navigating the public school system, much to his surprise he found himself studying math, physics, and computer science in college. He graduated with bachelor's degrees in all three from Oral Roberts University in 1991, and, finding that working as a waiter was not very exciting, he started a master's degree in math and/or physics. After mixing in several programming jobs (including video game programming), he obtained a master's degree in mathematics from Purdue University, Fort Wayne campus, in 1996. Certain that school was more fun than working, he drove to Purdue University, West Lafayette, to pursue a PhD in superstring theory, which is why seven years later this thesis is about error correcting codes. While chasing this lifelong dream of becoming a "scientist", or, equivalently, avoiding the private sector, he met the beautiful and brilliant Melissa Jo Wilson. They were (will be) married on April 26th, 2003. This document is the final hurdle to obtaining his PhD, which hopefully will be awarded in May 2003. With no more degrees to chase (on the horizon!), he entered the job market, and the rest is history.